Securing Your Journey
to the Cloud

THE "LURID" DOWNLOADER

TrendLabs™

By Nart Villeneuve & David Sancho

CONTENTS

Abstract

This report investigates a campaign of targeted malware attacks that has successfully compromised 1465 computers in 61 different countries. Based on the project path embedded in the malware, we have named this specific campaign "Lurid Downloader" although the malware is typically known as "Enfal". The majority of the victims are located in Russia and other members of the Commonwealth of Independent States (CIS). We were able to identify 47 victims that include numerous government ministries and diplomatic missions along with space-related government agencies, companies and research institutions in Russia and other members of the CIS along with a smaller amount of similar entities in Europe.

The threat actors behind "Lurid Downloader" launched 301 malware campaigns targeting entities in specific countries or geographic regions and tracked the success of each campaign by embedding a unique identifier in each instance of malware and associating it with specific victims. While some campaigns resulted in numerous victims, others were very specific and targeted resulting in only one or two victims. While previous Enfal activity has been typically associated with threat actors in China, it remains unclear who is behind the Lurid Downloader attacks.

Introduction

Prior to the highly publicized "Aurora" attack on Google in late 2009, which also affected at least 20 other companies, there was little public awareness regarding targeted malware attacks[1]. However, such attacks have been taking place for years and continue to affect government, military, corporate, educational, and civil society networks today. While such attacks against the U.S. government and related networks are now fairly well-known, other governments and an increasing number of companies are facing similar threats. Russia and other countries in the Commonwealth of Independent States are also being targeted and compromised. These countries have an expertise in the space industry and also have operations in oil & gas, mining and other industry areas that have been targeted by malware attacks in the past.

Malware attacks that exploit vulnerabilities in popular software in order to compromise specific target sets are becoming increasingly commonplace. These attacks are not automated or indiscriminate nor are they conducted by opportunistic amateurs. Known as targeted malware attacks, these attacks refer to computer intrusions staged by threat actors that aggressively pursue and compromise specific targets. Targeted malware attacks are typically part of broader campaigns, a series of failed and success compromises, by specific threat actors and not isolated attacks.

However, the specificity of the attacker's prior knowledge of the victim affects the level of targeting associated with a single attack. As a result, some attacks appear to be less precise, or "noisy", and are aimed at a broader community. Such "spear phishing" attacks are usually "directed toward a group of people with a commonality" as opposed to a specific target but are useful for gaining an initial foothold in a future target of interest[2].

The malware used in the "Lurid Downloader" attacks is commonly known as "Enfal" and it has been used in targeted attacks as far back as 2006[3]. In 2008, Maarten Van Horenbeeck documented a series of targeted malware attacks that made use the Enfal Trojan to target non-governmental organizations, non-governmental organizations (NGOs) as well as defense contractors and U.S. government employees[4]. In 2009 and 2010, researchers from the University of Toronto published reports on two cyber-espionage networks known as "GhostNet" and "ShadowNet" that included malware and command and control infrastructure connected with the Enfal Trojan[5]. The domain names used by Enfal as command and control servers are, according to U.S. diplomatic cables leaked to Wikileaks, linked to a series of attacks known as "Byzantine Hades." According to these leaked cables, the activity of this set of threat actors has been ongoing since 2002 and is known as "Byzantine Hades", and there are subsets of this activity known as "Byzantine Anchor," "Byzantine Candor" and "Byzantine Foothold"[6]. However, it is important to note that other than the use of Enfal itself, there appears to be several distinct sets of command and control infrastructure in use and the relationship among the threat actors operating these separate infrastructures remains unclear.

The "Lurid Downloader" attacks appear to be another separate, but related Enfal network with a geographic focus. While there is clear evidence that the Tibetan community is also target, the victims of this attack are concentrated in Russia and other CIS countries. Numerous embassies and government ministries have been compromised as well as research institutions and agencies related to the space industry.

Our investigation began with an analysis of the "Lurid Downloader" malware. Our objective was to document its functionality and map out its command and control network. While this malware family is well known, there appear to be various associated threat actors using it to compromise targets in various geographic locations. Similar versions of this malware have been used to target both the U.S. government and NGO's in the past. We could find no direct links between this particular command and control network and the previously discovered ones; we believe that it is most likely a separate, but related network as they appear to each have a regional focus.

We uncovered a command and control network that consists of 15 domains names and 10 IP addresses. We were able to retrieve a listing of the compromised computers connecting to these servers. In total, we found 1465 unique hosts (Hostname + Mac address as stored by the C&C) with 2272 unique external IP addresses connecting to the command and control network primarily from Russia (1063), Kazakhstan (325) and Ukraine (102) along with numerous other countries in the CIS (former Soviet Union).

We were able to use reverse DNS and WHOIS lookups to determine the identity of 47 compromised hosts. From the victims we were able to identify, there were concentrations of government ministries and diplomatic missions as well as space-related government agencies, companies and research institutions.

We found that the attackers embedded campaign codes inside the malware they propagated in order to keep track of the success of their campaigns. In total, we found 301 campaign codes and there are high concentrations of victims within a single country for each instance of the malware campaign indicating that the distribution of the malware is targeted at specific countries or regions. In addition, nearly 60% of the campaigns only affected 1 or 2 victims indicating the precision with which the malware campaigns were conducted.

[1] For the attacks on Google, see http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

[2] http://www.cisco.com/en/US/prod/collateral/vpndevc/ps10128/ps10339/ps10354/targeted_attacks.pdf

[3] http://about-threats.trendmicro.com/ArchiveMalware.aspx?language=us&name=TROJ_SHARP.R

[4] http://events.ccc.de/congress/2007/Fahrplan/attachments/1008_Crouching_Powerpoint_Hidden_Trojan_24C3.pdf , http://isc.sans.org/presentations/SANSFIRE2008-Is_Troy_Burning_Vanhorenbeeck.pdf, http://isc.sans.edu/diary.html?storyid=4177

[5] While the domain names are present in the GhostNet report, they are not part of GhostNet but a completely different network of command and control servers that are actually associated with Enfal. http://www.nartv.org/mirror/ghostnet.pdf and http://www.nartv.org/mirror/shadows-in-the-cloud.pdf

[6] http://wikileaks.org/cable/2009/04/09STATE32025.html http://cablesearch.org/cable/view.php?id=08STATE116943 and http://www.reuters.com/article/2011/04/14/us-china-usa-cyberespionage-idUSTRE73D24220110414

Attack Vector

In a typical targeted malware attack, a target typically receives a socially engineered message – such as an email or instant message – that encourages the target to click on a link or open a file. The links and files sent by the attacker contain malicious code that exploits vulnerabilities in popular software such as Adobe Reader (e.g. pdf's) and Microsoft Office (e.g. doc's). The payload of these exploits is malware that is silently executed on the target's computer. This allows the attackers to take control of the computer and obtain data from it. The attackers may then move laterally throughout the target's network and are often able to maintain control over compromised computers for extended periods of time. Ultimately, the attacks locate and ex-filtrate sensitive information from the victim's network.

In this case, the delivery mechanism used was an email with a malicious PDF as an attachment. The email had no content, just a subject line and an attachment. The email message was spoofed to appear to be from ohhdl@dalailama.com, the Office of the Dalai Lama and had a subject of “Tibetan Losar Event on 6 March 2011”. It also contained an attachment named “LOSAR FLYER_edited-3.pdf”.

The email was sent using an email provider called Gawab (gawab.com) which is popular in the Middle East. The server used was info3.gawab.com (66.220.20.18) and the email address was emb107@gawab.com. The originating IP address was: 96.46.11.88 (INTERNETXTUSA). While this IP address is assigned to the US, it is used by a VPN provider in China[7].

If the attached PDF is opened with older versions of Adobe reader, malicious code is executed that drop malware on the target's system. The malware then connects to a command and control server under the attacker's control. At this time, the target's computer is compromised and under the full control of the attackers.

[7] http://www.ldvpn.cn/us-dongtai.html

Malware

MD5	File Name	Detection
322fcf1b134fef1bae52fbd80a373ede	LOSAR_FLYER_edited-3.pdf	TROJ_PIDIEF.SMZX

This PDF contains a JavaScript stream that exploits the util.printd vulnerability (CVE-2009-4324) that affects Adobe Reader 9.x (before 9.3) and 8.x (before 8.2).

MD5	File Name	Detection
84d24967cb5cbacf4052a3001692dd54	ctfmon.exe	TROJ_MECIV.A

This PDF contains a JavaScript stream that exploits the util.printd vulnerability (CVE-2009-4324) that affects Adobe Reader 9.x (before 9.3) and 8.x (before 8.2).

MD5	File Name	Detection
3447416fbbc65906bd0384d4c2ba479e	mspmsnsr.dll[chars]	TROJ_MECIV.A

After successful exploitation, two malware components are created. One is a dropper (ctfmon.exe) that installs a windows service. The service loads the dropped dll file mspmsnsr.dll<long string of characters>. The malicious Windows service stores its configuration settings in the registry:

HKLM\SYSTEM\CurrentControlSet\Services\WmdmPmSp\Parameters

This malware identifies itself as version 2.14. During the course of our investigation, we discovered another version of the malware that identifies itself as version 2.15.

MD5	File Name	Detection
856de08a947a40e00ea7ed66b8e02c53	isssync.exe	WORM_OTORUN.TMP

Instead of a Windows service, version 2.15 is just a single executable that copies itself to the system folder and ensures persistence by changing the common start folder of windows to a special one it creates. It then copies all the usual auto-start items there, as well as itself. The existence of this folder is constantly checked and redone if the user or any program switches it back to normal.

The Trojan collects information from the computer and sends it via HTTP POST. The information it collects is the following:

- Computer name
- MAC address
- computer OS and version
- IP address and codepage
- language of the operating system.

It constantly communicates with a C&C server to perform certain info-stealing tasks. The main feature of the Trojan is that all communication is started by the client by http. Firewalls and other security devices will never see any communication from outside in. Even the interactive command line is built this way so everything is done from the inside out. The communication is always encrypted although it's a simple XOR single-byte encryption. This means that network security devices won't readily see anything suspicious going on.

Communication with the Command and Control Server

When malware is executed on the target's system it "checks in" with one or more servers under the control of the attackers. Command and control mechanisms allow the threat actors to confirm that an attack has succeeded in addition to supplying them with some information about the target's computer and network. From here on, the client communicates back to the control server expecting a command, allowing the attackers to issue commands to the compromised target.

All of the connections to the command and control servers use the HTTP protocol and request specific URL paths. On startup, the malware connects to the command and control server and requests the path "/trandocs/mm/" (the path may differ with other samples, for example "httpdocs/mm/ or /iupw82/netstate"). This appears to be a LOGIN connection and the server always responds with "123". The data transmitted to the command and control server consists of the following:

Encrypted Password/<hostname>:<MAC>/<ip address>
<OS name>
<codepage>:<locale>
<actual exe name>
<campaign name>
<y/n> (sys32time.ini exists? Is it 1Mb or bigger?)
<y/n> (ipop.dll exists?)
<y/n> (always n in our samples)
<malware version> (2.14 or 2.15)

The encrypted password at the beginning of the LOGIN packet only appears on version 2.15. The sample we analyzed contains the password "hallelujah" and it is encrypted with "ADD +FAh". The earlier version, 2.14, does not contain a password at all.

After the initial connection, the malware makes two kinds of connections to the command and control server every 2 minutes. The first connection is a KEEPALIVE connection to the URL path "/cgl-bin/Owpq4.cgi". The malware posts information to the command and control server that identifies the compromised machine: OS and version, "campaign ID" and malware version. The second connection is an ASKCMD connection to a URL with the path "/trandocs/mm/ <machine_name>:<MAC address>/Cmwhite". The contents of "Cmwhite" contain commands that are sent by the attackers to the compromised computer. The range of possible commands will be discussed below.

When the command file, "Cmwhite" is downloaded, the malware first acknowledges the receipt of the command by issuing an ACKCMD connection to "/cgl-bin/Clnpp5.cgi". Once the command is interpreted and performed, the malware issues a CMDDONE request to "/cgl-bin/Rwpq1.cgi". It contains the results of the command and, if relevant, a result code that indicates any error encountered. When there is no command set by the attackers for the victim computer, the command and control server returns a "404 NOT FOUND" error page. This is never interpreted correctly as a command and therefore ignored.

Commands

The command packet that is contained within the "Cmwhite" response is encrypted. In the samples we analyzed, it is encrypted with XOR 45h. Other communication packets observed suggest that there are other keys in use but they are always a single byte. Once decrypted, this is what a command packet contains:

First two bytes: 40 40. (This is just a magic number).
Third byte: Command code.
Fourth byte: Return code. (This only used in the CMDDONE packet to indicate error/success).
From the Fifth byte on, the command carries parameters, which vary depending on the nature of the command.

The range of commands available to the attackers that are enumerated below demonstrate the level of control the attackers have over their victims. In addition to functionality that allows the attackers to send and receive files, they are able to activate an interactive remote shell on compromised systems.

Range of commands		
Command 01	ECHO	It echoes back the word contained in bytes 5 and 6. There's another parameter, which is supposed to contain the string "ibme54". If this is right, it keeps an internal counter of how many of these ECHO packets, it has received.
Command 02	IPOP LOAD CHECK	It checks if the previous check for the file c:\windows\system32\ipop.dll was successful. It returns a y/n condition.
Command 03	SEND FILE	When the client receives this command, it retrieves a file and sends it to the C&C server. The filename is a parameter in the command packet.
Command 04	RECV FILE	This command has two parameters, the filename and the data. The client creates the file with the data in the packet. It does this by constantly communicating with a Ufwhite URL. This URL is accessed repeatedly in order to keep receiving chunks of the data file and appending it to the file. When there's no more data, the file is closed and operation is finished. After each packet is correctly received, the client sends a report packet to Clnpp5.cgi specifying that it was Ufwhite who started this operation.
Command 05	CMDEXEC	It accepts a single command and executes it in the victim system.
Command 06	DELETE FILE	It accepts a filename string as a parameter. It deletes the file.
Command 07	MOVE FILE	It accepts two filenames. It moves the file from source to target destination.
Command 09	LS	When the client receives this command, its proceeds to list the files within a specified directory and sends the list back in a response packet.
Command 0A	INTERACTIVE MODE	When the client receives this command, it stays in interactive mode. It starts connecting to Clnpp5.cgi expecting a command. These commands are then executed and error codes sent straight away until an "exit" command is received. The interactive commands have a special tag to set them apart from regular commands. This tag is "1234". The way this interactive system is implemented is the following: The command is run in the same way as command 05 but the output is redirected to a file (c:\Documents and Settings\<user>\SendTo\msacm.dat). The contents of the file are then sent in the return packet to Clnpp5.cgi. Once the "exit" command has been received, this mode is interrupted. While this mode is going on, the Trojan still sends keepalive and regular command requests packets.

Command 0B	MKDIR	The client creates a directory
Command 0E	TERMINATE PROCESS	The client tries to terminate a given thread in the system.
Command 10	EXEC NFAL	When this command is received, the client tries to execute the file c:\windows\system32\nfal.exe. This file does not exist on an infected system normally so it must be a placeholder for a command file uploaded to the victim.
Command 40	PING	When this command is received, the Trojan just sends back an empty packet with a success code condition.

Tool Marks

The terms "tool marks" refers to characteristics contained within malware that indicate that they are part of the same campaign or related to specific threat actors[8]. In this case, the attackers left the PDB path in the malware samples we analyzed which indicate the name of the project:

e:\programs\LuridDownLoader\LuridDownloader for Falcon\DllServiceTrojan\Release\DllServiceTrojan.pdb
e:\programs\LuridDownLoader\LuridDownloader for Falcon\ServiceDll\Release\ServiceDll.pdb

We named this campaign of targeted attacks "Lurid DownLoader" based on the project name the attackers have given to their own malware.

[8] http://mobile.darkreading.com/9287/show/571d636618a7ba35b7e9bae872fc5bfd&t=ebba8420c261102635de4d20bdd772f2

Command and Control Infrastructure

Attackers often maintain a network of command and control servers, not just a single one. Often, the malware used in targeted attacks contains one or more command and control locations. By linking together the domain names that are present in related malware samples, along with domain names registered by the same email address and domain names hosted on the same web servers we were able to map out the command and control infrastructure of the attackers.

In total, we found 15 domain names associated with the attackers and 10 active IP addresses. The domain names were registered by two different email addresses "bruce_tuner@yahoo.com" and "icqmaster@163.com".

DOMAINS	REGISTRATIONS
mailru-vip.com yandex-vip.com google-officeonline.com office-helppane.com foxit-pro.com ymail-vip.com ymail-pro.com yandex-pro.com google-office.com mailru-pro.com	xiaohu wang bruce_tuner@yahoo.com +86.01089464156 fax: +86.01089464156 bei jing shi beijing beijing 102600 CN
hoticq.com redhag.com zadhc.com lasmail.com hotoicq.com	jason bush icqmaster@163.com +86.01062311307 fax: +86.01062311307 No.20 Xueyuan Road,Haidian District,Beijing beijing beijing 100083 CN

Rather than use the "root" domains, the attackers use a variety of sub-domains. These various sub-domains resolve to 10 different IP address spread across 3 different IP address ranges assigned to 2 providers: Krypt Technologies in the U.S. and UK2/100mb in the U.K.

Additional malware samples that connect to this command and control infrastructure are:

MD5	Domain	IP ADDRESS
ed69041fbe470fe0f2c1fd837efcb6e7	ace.mailru-vip.com home.mailru-pro.com xphlp.ymail-vip.com	173.212.195.216
d66948e4e90baff08d24c77c93788597	ace.mailru-vip.com home.mailru-pro.com xphlp.ymail-vip.com	173.212.195.216
2d93cbe969d3b5f02d4f9f1a3eb39b85	ace.mailru-vip.com home.mailru-pro.com xphlp.ymail-vip.com	173.212.195.216
465ca2eef82b412949eeaa9fa3cc5c75	setup.mailru-vip.com	109.123.126.143
e1833932053171da15c60e6c2fca708a	superkiller.mailru-vip.com sexinsex.ymail-vip.com	109.123.126.156
e38ccff8e7fb922fe48b54b4032fec50	setup.mailru-vip.com	109.123.126.143 (184.95.36.75)
744670ca4531f7ceb72a75ae456e8215	microsoft.office-helppane.com	109.123.126.151
f0f31112af491f56af7cc0802ba96c0f	microsoft.office-helppane.com win.foxit-pro.com update.ymail-vip.com	109.123.126.151 106.123.126.151
2a21eb36cc2a0a24149a4821aa328b7b	microsoft.office-helppane.com	109.123.126.151
5403e0bda1db72e5e862e9169db4e1d7	led.office-helppane.com	174.139.13.122 (184.95.36.75)
57d99d67c3e8987e812c9332d6774794	press.foxit-pro.com	
963e39d8675b5bb3d2f4e6da45c51bb0	press.mailru-pro.com	(184.22.240.174)
166d6cd28c9df20c30fed220a3132345	press.ymail-pro.com	46.23.67.226
89b98f66650cb29d0926713fda3b5bbc	press.ymail-pro.com	46.23.67.226 (184.22.251.12)

d8815fe64eb5321add412554908da28a	help.lasmail.com	109.123.126.157
22caf76a780c54ddce7fa139100fa54e	mail.lasmail.com	109.123.126.157 (58.64.149.29)
140c69ea9a963100e75497b33820f1da	help.lasmail.com	109.123.126.157 (204.12.197.70)
8f65204d8440b7be2b52908e35d19124	mail.lasmail.com	109.123.126.157 (58.64.149.29) (204.12.197.70)
f993d4cabe5021c96d6a80192f142dca	support.hotoicq.com	109.123.126.157
74bdabd1077d640f7d21c6cfb14a0348		204.12.197.70
22caf76a780c54ddce7fa139100fa54e	mail.lasmail.com	109.123.126.157 (58.64.149.29)
140c69ea9a963100e75497b33820f1da	help.lasmail.com	109.123.126.157 (204.12.197.70)
8f65204d8440b7be2b52908e35d19124	mail.lasmail.com	109.123.126.157 (58.64.149.29) (204.12.197.70)
f993d4cabe5021c96d6a80192f142dca	support.hotoicq.com	109.123.126.157
74bdabd1077d640f7d21c6cfb14a0348		204.12.197.70

Compromised Organizations

After mapping out and monitoring the command and control network used in this campaign we were able to retrieve a listing of the compromised computers connecting to these servers. This list of compromised computers contains 1465 unique hosts (Hostname + Mac address as stored by the C&C) with 2272 unique external IP addresses connecting to the command and control network primarily from Russia (1063), Kazakhstan (325) and Ukraine (102) along with numerous other countries in the CIS (former Soviet Union). There were also significant numbers of compromises in Vietnam, India, Mongolia and China. In total, there were victims in 61 different countries.

The data covers compromised computers that connected to the command and control servers in June and July 2011. The top 10 countries of victims (based on the 2272 IP addresses) are:

RU	1063
KZ	325
UA	102
VN	93
UZ	88
BY	67
IN	66
KG	49
MN	42
CN	39

Malware Campaigns

As noted earlier, there is a unique identifier built in to instances of the malware sent out by the attackers that allows them to keep track of the computers compromised by specific campaigns. In total, we found 301 campaign codes. This means that the attackers sent out at least 301 different instances of the "Lurid Downloader." There are high concentrations of victims within a single country for each instance of the malware campaign indicating that the distribution of the malware is targeted at specific countries or regions.

Campaign	Count	Countries
strong	668	All 68 of the compromised counters were in Vietnam.
ejun0708	63	5 in Russia, 3 in Ukraine and 1 each in Czech Republic, Kazakhstan, Switzerland, Tajikistan and Belarus
ejun0614	42	27 in Russia, 3 in China, 3 in Kyrgyzstan, 2 in Tajikistan and 1 each in UK, US, S. Korea, Czech republic, Pakistan, Germany and Kazakhstan.
strongNewDns	34	All 34 of the compromised counters were in Vietnam.
ejun0509	32	31 in Russia, 1 in Ukraine
ejun0511	29	21 in Russia, 4 in Ukraine, 2 in Kazakhstan, and 1 each in Czech Republic and Azerbaijan
7-28	28	24 in Vietnam and one each in UAE, Cambodia ,Thailand and China
ejun0503	25	23 in Russia and 1 each in Ukraine and Czech Republic
0dayaug12.exe	22	20 in Belarus and 2 in Kazakhstan
C:\WINDOWS\system32\desp.exe	22	12 in US, 5 in Russia, 3 in The Netherlands, and 1 each in Switzerland and the European Union.

There were also specific campaigns that affected a very small number of victims. In fact, nearly 60% (59.4%) of all the campaigns affected only 1 or 2 victims. There were 115 campaigns that only compromised 1 victim and 64 campaigns that only compromised 2 victims. This indicates the precision in malware campaigns that target specific entities.

Noteworthy Compromised Organizations

We were able to use reverse DNS queries and WHOIS lookups to determine the identity some of the compromised hosts. There are high profile diplomatic organizations that have been compromised as well as agencies relating to space and research institutions.

Country	Sector	Date	Camapign
France	GOV	Sat Jun 18 10:22:22 2011	0dayjun14.exe
Switzerland	GOV	Mon Jul 11 11:28:02 2011	LOGO076
UK	MEDIA	Thu Jun 16 08:18:44 2011	0dayapr13.exe
Germany	SPACE	Mon Jun 20 09:43:48 2011	6-7
Spain	SPACE	Mon Jul 4 11:38:35 2011	6-27
Russia	GOV	Tue Jun 7 12:15:34 2011	lh0603hy
Russia	GOV	Mon Jul 11 07:17:46 2011	ejun0708
Russia	GOV	Tue Jun 28 00:54:16 2011	110608
Russia	SPACE/GOV	Wed Jul 13 04:21:20 2011	aoo526pdf
Russia	SPACE	Wed Jul 13 07:14:38 2011	winupdate712
Russia	SPACE	Mon Jul 25 08:43:40 2011	6-7
Russia	SPACE	Wed Jul 13 02:45:59 2011	coo328xls
Russia	RESEARCH/GOV	Wed Jul 13 06:06:06 2011	aoo0516pdf
Russia	RESEARCH	Wed Jul 20 12:01:00 2011	6-27
Russia	RESEARCH	Mon Jul 11 07:38:14 2011	winupdate0706
Russia	RESEARCH	Tue Jun 14 08:09:23 2011	110303
Russia	RESEARCH	Wed Jul 13 02:46:24 2011	coo0609doc
Russia	RESEARCH	Wed Jul 13 02:47:33 2011	sat0608old
Russia	RESEARCH	Tue Jun 14 02:49:58 2011	winupdate
Russia	RESEARCH	Tue Jun 14 02:38:52 2011	satellite0608
Russia	MEDIA	Tue Jun 14 04:25:12 2011	ejun0125
China (Russia)	BUSINESS	Tue Jun 7 13:17:39 2011	lh0603hy
Russia	BUSINESS	Tue Jun 14 07:28:25 2011	z11apr27aboky
Russia	GOV	Tue Jun 14 11:49:35 2011	z10nov23k
Russia	POLITICAL PARTY	Tue Jun 14 14:05:24 2011	LOGO69
Russia (Ukraine)	GOV	Mon Jul 4 10:36:46 2011	LOGO704
Turkmenistan	GOV	Mon Jun 13 07:28:59 2011	0dayjun09.exe
Kyrgyzstan	GOV	Mon Jun 13 07:33:12 2011	0dayjun09.exe
Kazakhstan	GOV	Mon Jun 13 06:06:47 2011	0daydec08.exe
Kazakhstan	GOV	Mon Jun 27 15:15:42 2011	smross.exe

Ukraine	GOV	Wed Jun 22 15:43:26 2011	LOGO615
Kazakhstan	GOV	Mon Jun 13 06:06:47 2011	0daydec08.exe
Kazakhstan	GOV	Mon Jun 27 15:15:42 2011	smross.exe
Ukraine	GOV	Wed Jun 22 15:43:26 2011	LOGO615
Belarus	GOV	Thu Jul 14 17:58:48 2011	0dayaug12.exe
Germany (Kazakhstan)	GOV	Tue Jun 21 10:07:49 2011	LOGO621
Austria (Kyrgyzstan)	GOV	Mon Jun 13 09:34:45 2011	LOGO524
Russia (Tajikistan)	GOV	Tue Jun 7 12:00:03 2011	lh0526w.exe
Kazakhstan	GOV	Thu Jul 7 05:44:34 2011	LOGO0705
Kyrgyzstan (Kazakhstan)	GOV	Tue Jul 12 10:57:17 2011	z10dec09UP.exe
Kazakhstan (China)	GOV	Tue Jun 14 08:58:53 2011	LOGO69
Kazakhstan	RESEARCH	Thu Jun 16 08:24:31 2011	LOGO616
Belarus	RESEARCH	Wed Jul 13 05:37:40 2011	services712
Armenia	RESEARCH	Fri Jun 24 07:25:18 2011	LOGO624
Kazakhstan	MEDIA	Mon Jun 13 08:17:29 2011	z10nov25knb
Vietnam	GOV	Sun Jul 3 09:06:57 2011	strong
China	BUSINESS	Sun Jun 12 06:02:11 2011	lh0517e.exe
Uzbekistan	GOV	Tue Jun 14 05:41:09 2011	0dayjan27
Vietnam	GOV	Tue Aug 2 12:57:36 2011	7-28

Data Ex-Filtration

While we were unable to recover the data obtained by the attackers, we were able to collect some of the command issued by the attackers that hint at their objectives. We found that the attackers often issued the “LS” command to send a directory listing from specific directories on the compromised computers back to the command and control server. We also observed the use of the “SEND FILE” that ordered the compromised computers to compress, split and upload specific files (.rar, .xls, .doc) to the command and control server. However, we were unable to recover the ex-filtrated data.

Attribution

Determining who is ultimately behind targeted malware attacks is difficult as it requires a combination of technical and contextual analysis and the ability to connect disparate pieces of information together over a period of time. Moreover, any one researcher typically does not necessarily have all these pieces of information and must interpret the available evidence. Too often, the determination of attribution is based on easily spoofed evidence such as IP addresses. While many of these attacks are attributed to China, in this case, the IP addresses of the command and control servers were located in the United States and the United Kingdom. However, the registration information of the domain names used indicates that the owners are in China. In either case, the information is not difficult to manipulate.

The use of "Enfal", the family of malware to which "Lurid Downloader" belongs, has been historically linked with threat actors in China. In this case, the attack vector that we were able to analyze was related to the Tibetan community which indicates an association with China. However, China was also a victim of "Lurid Downloader."

Conclusion

In this report we have analyzed targeted malware attacks that have compromised sensitive locations in Russia, CIS countries and around the world. The focus of the attacks appears to be on government networks and diplomatic missions as well and research institutions and space related agencies. We found that the attackers engaged in over 300 campaigns and kept careful records of their victims and to what campaign compromised them. Our analysis of the campaigns reveals that attackers engage in attacks that target communities in specific geographic locations as well extremely targeted campaigns that only affect one or two victims.

The precise nature of targeted malware attacks increases the difficulty of defense. With significant reconnaissance, and possibly information gained from previously successful incursions into the target's network, the threat actors behind targeted malware attacks are able to customize their attacks to increase the probability of success. Therefore, defenses against targeted malware attacks need to focus on detection and mitigation and not simply on prevention.

Through the exposure of the "Lurid Downloader" network, we aim to enable a better understanding of the extent and frequency of such attacks as well as the challenges that targeted malware attacks pose for traditional defenses. Defensive strategies can be dramatically improved by understanding how targeted malware attacks work as well as trends in the tools, tactics and procedures of the threat actors behind such attacks. By effectively using threat intelligence derived from external and internal sources combined with security tools that empower human analysts, organizations are better positioned to detect and mitigate targeted malware attacks.

TREND MICRO™

Trend Micro Incorporated is a pioneer in secure content and threat management. Founded in 1988, Trend Micro provides individuals and organizations of all sizes with award-winning security software, hardware, and services. With headquarters in Tokyo and operations in more than 30 countries, Trend Micro solutions are sold through corporate and value-added resellers and service providers worldwide. For additional information and evaluation copies of Trend Micro products and services, visit our website at www.trendmicro.com.

TRENDLABS℠

TrendLabs is Trend Micro's global network of research, development, and support centers committed to 24 x 7 threat surveillance, attack prevention, and timely and seamless solutions delivery.