

RSA RESEARCH

TERRACOTTA VPN

Enabler of Advanced Threat Anonymity

August 4, 2015

Content and liability disclaimer

This Research Paper is for general information purposes only, and should not be used as a substitute for consultation with professional advisors. EMC has exercised reasonable care in the collecting, processing, and reporting of this information but has not independently verified, validated, or audited the data to verify the accuracy or completeness of the information. EMC shall not be responsible for any errors or omissions contained on this Research Paper, and reserves the right to make changes anytime without notice. Mention of non-EMC products or services is provided for informational purposes only and constitutes neither an endorsement nor a recommendation by EMC. All EMC and third-party information provided in this Research Paper is provided on an "as is" basis.

EMC DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, WITH REGARD TO ANY INFORMATION (INCLUDING ANY SOFTWARE, PRODUCTS, OR SERVICES) PROVIDED IN THIS RESEARCH PAPER, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. Some jurisdictions do not allow the exclusion of implied warranties, so the above exclusion may not apply to you.

In no event shall EMC be liable for any damages whatsoever, and in particular EMC shall not be liable for direct, special, indirect, consequential, or incidental damages, or damages for lost profits, loss of revenue or loss of use, cost of replacement goods, loss or damage to data arising out of the use or inability to use any EMC website, any EMC product or service. This includes damages arising from use of or in reliance on the documents or information present on this Research Paper, even if EMC has been advised of the possibility of such damages

Copyright © 2015 EMC Corporation. All Rights Reserved.

Use, copying, and distribution of any EMC software described in this publication requires an applicable software license. RSA and the RSA logo are registered trademarks or trademarks of EMC Corporation in the United States and other countries. All other products and/or services referenced are trademarks of their respective companies. Published in the USA. August 4, 2015

EXECUTIVE SUMMARY	5
BACKGROUND	5
WHAT IS TERRACOTTA VPN?.....	5
TERRACOTTA VPN COMPONENTS.....	6
BEHIND THE TERRACOTTA NODES	7
BEHIND TERRACOTTA NODES: THE VICTIMS.....	9
TERRACOTTA WINDOWS SERVER ENLISTMENT MODUS OPERANDI.....	9
THE ECONOMICS OF HACKING FOR A PROFIT	10
VPN NODES THAT DON'T "LOOK LIKE" VPN NODES.....	11
WHO USES TERRACOTTA VPN?	12
SUSPECTED NATION STATE SPONSORED CAMPAIGNS LEVERAGING TERRACOTTA VPN	12
TERRACOTTA VPN LEVERAGED FOR PHISHING AND ATTEMPTED EXPLOITATION OF A DEFENSE CONTRACTOR	12
SHELL_CREW	14
TERRACOTTA VPN BREAKDOWN.....	15
DETECTION	15
DETECTING NODE ENLISTMENT ACTIVITY	15
DETECTING NODE USE IN ATTACKS.....	15
DETECTING USE OF TERRACOTTA VPN RESOURCES.....	16
DETECTING TERRACOTTA ASSOCIATED MALWARE.....	16
DETECTING TERRACOTTA ACTIVITY IN RSA SECURITY ANALYTICS AND RSA ECAT	23
DETECTING TERRACOTTA MALWARE USING RSA SECURITY ANALYTICS AND ECAT.....	25
PREVENTION.....	32
ATTRIBUTION AND PATTERN OF LIFE	32
CONCLUSIONS	33

APPENDIX	33
AVAILABLE TO INDUSTRY PARTNERS UPON REQUEST	33
AUTHORS	33

EXECUTIVE SUMMARY

In this report, RSA Research explores in depth a malware-supported VPN network, known internally to RSA as Terracotta.

Terracotta is an active launch-platform for APT activities of Shell_Crew / DeepPanda and other APT actors, used to obscure the origins of the threat actors' malicious activities. It is ensnaring a new class of victims (legitimate commercial and government entities, unknowingly serving VPN nodes and bandwidth) into larger-scale APT cases. Fortunately, enlistment in the Terracotta network is readily preventable by using well-established cybersecurity practices. Detection and mitigation for enlisted systems is also quite feasible.

Terracotta is commercially marketed in the People's Republic of China (PRC) under several different brand names. VPN services are quite marketable in China as a means to anonymously traverse government internet censorship. Terracotta's malicious methods for acquiring nodes and theft of bandwidth likely derives substantial cost-savings for its operators.

Having provided Terracotta VPN indicators to trusted partners, RSA has received multiple reports of (and since observed) suspected nation-state sponsored campaign activity originating from Terracotta VPN IP addresses. Targets appear to have included Western governments and several commercial entities. By using Terracotta VPN, advanced threat actors appear to originate from seemingly benign sources. Blocking, restricting, or detecting by IP address indicators is difficult because new nodes (hosted in legitimate organizations) are being continuously added.

This report by RSA Research may represent the first exposure of a PRC-based VPN operation that maliciously, efficiently and rapidly enlists vulnerable servers around the world. It is the first time RSA Research has seen Shell_Crew / DeepPanda and other similar APT actors using such networks for anonymization and obfuscation.

BACKGROUND

Virtual Private Networks (VPN) are very popular. They are part and parcel for almost every enterprise network, especially those with remote employees. Aside from VPNs for enterprises, there are many reputable commercial VPN services that offer low-cost, reliable service to individual users. These users employ VPNs for reasons that might include connection security, protection of private data, online gaming acceleration, and bypassing service provider restrictions. VPNs are also used by cyber criminals, as it allows them to obscure their true source location. When a commercial VPN service provider uses resources such as servers and copious bandwidth stolen or repurposed from unsuspecting victims for purposes of profit, analysis and reporting are in order. In this report, RSA Research exposes one such operator doing business with multiple VPN brand names marketed primarily in the People's Republic of China (PRC). Operating with more than 1500 end nodes around the world, RSA Research has confirmed that at least thirty of the host systems are compromised Windows servers that were "harvested" without the victims' knowledge or permission. The operators behind Terracotta VPN continue their broad campaign to compromise multiple victim organizations around the world. RSA Research is reporting on the associated VPN operator because:

- There is evidence of compromise of multiple victim organization systems around the world,
- There is evidence of illicit installation of software and malicious remote access tools on the victims' servers, and
- There is evidence of theft of victims' resources and bandwidth to serve clients (including advanced threat actors) with a high-performance anonymity service.

NOTE: There are two classes of victims described and referred to in this report. Most of the references to victims are of those unknowingly enlisted into the Terracotta VPN service, as outlined above. A second class of victims, APT targets, have been targeted by other actors who are using Terracotta for anonymization and obfuscation. Throughout this report, we specifically refer to APT-victims accordingly, while leaving the generic 'victim' designation for the Terracotta nodes.

WHAT IS TERRACOTTA VPN?

Terracotta VPN is the name used by RSA Research to describe the dynamically-maintained conglomerate of multiple VPN "brand" names marketed on Chinese-language websites. The websites are principally linked by common domain name registrant email addresses and are often hosted on the same infrastructure with the same basic web content.

TERRACOTTA VPN COMPONENTS

There are several high-level components to the Terracotta VPN system.

- **WEBSITES:** The most visible Terracotta VPN components are the websites that market the service and the specific brands associated with Terracotta VPN. VPN users can download the software clients, obtain trial credentials, change credentials for their paid accounts, and add credit to paid accounts from these websites.
- **CLIENT SOFTWARE:** The client software is another common Terracotta VPN element. The client interfaces are skinned with images and logos consistent with their corresponding websites. The client software is principally developed by a legitimate software vendor, according to the application's file properties and indicative by the domains contacted by the client when the user logs-in.
- **CLIENT SOFTWARE AUTHENTICATION:** Closely-tied to the client software is the central client authentication system, by which clients use credentials to authenticate into the client software. Upon successful login, the client software will check for updates and download the latest set of global VPN nodes.
- **COMMON VPN NODES:** The dynamic set of 1500+ VPN nodes is another component. These nodes are shared among most of the Terracotta VPN brands and, most notably, link the different elements of the Terracotta VPN ecosystem. The roster of nodes is updated by the various software clients during each login sequence. Figure 1 illustrates the relationships between the Terracotta VPN components and the client VPN-tunneling sequence.
- **USER AUTHENTICATION;** The final component is the central Radius-compatible, Internet Authentication Service (IAS) directory that authenticates the user account credentials with the VPN node.

The steps are:

1. The Terracotta user establishes an account; obtains credentials and client software from one of the Terracotta brand websites.
2. The user signs into the client UI, which authenticates the client credentials against the central client authentication system.
3. The software client will then populate with an updated roster of VPN nodes.
4. Once the user selects a VPN node, the node will authenticate the user credentials with the distributed IAS directory.
5. Following successful authentication, the Point-to-Point Tunneling Protocol (PPTP) or Layer-Two Tunneling Protocol (L2TP) session is established.

At this point the user has successfully tunneled to the Internet through the Terracotta VPN end point.

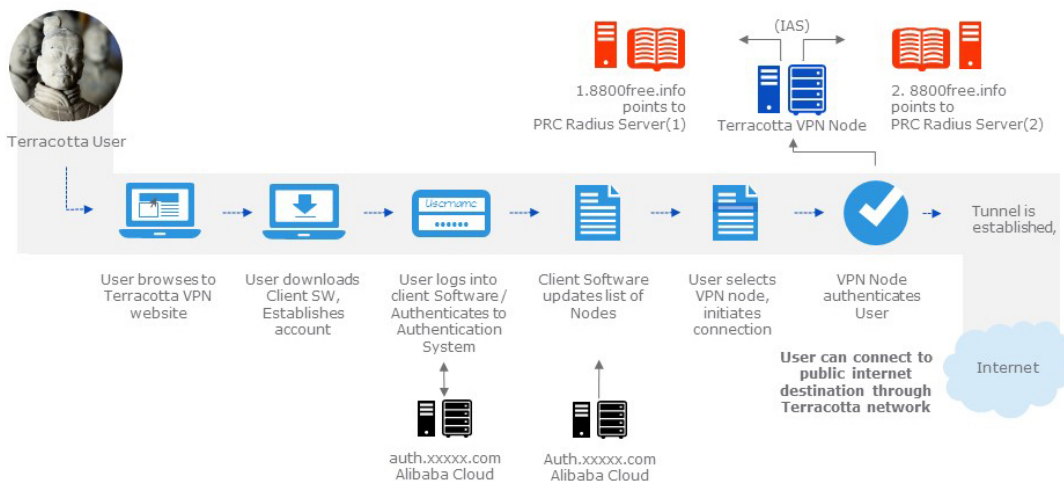


Figure 1. How Terracotta VPN Works

BEHIND THE TERRACOTTA NODES

Where do the various Terracotta VPN providers obtain the resources to build such a vast VPN network? Out of 1500+ common VPN nodes, it is possible that some servers or appliances were legitimately obtained and leased by the Terracotta VPN operators. We will describe how others were clearly compromised. RSA Research proposes three possible candidates (three devices) encompassing 557 IP addresses. We believe these devices are the best possible candidates for legitimate lease by the Terracotta VPN perpetrators for the following reasons:

1. Massive multi-homing: The minimum quantity of IP addresses per suspected-legitimately-leased-device is 51. Terracotta services are marketed as very cost-effective, offering availability of a large VPN network for approximately \$3/month. Massive multi-homing of a single device is apparently a method for inflating the appearance of the network. A Terracotta VPN client pings and displays all available nodes, noting both the date each node came online and its current response-time. However, while the network may appear to offer multiple new nodes on a given day, nodes with the same enlistment date and similar response-times actually indicate a multi-homed device. Further, network analysis shows the VPN clients usually connect to only a single IP address assigned to each massively multi-homed device. This may result in lower maintenance overhead, and indicates that the Terracotta VPN operator knows full-well that there is just one device behind the large pool of available nodes. And while there is no performance benefit from having the VPN clients ping multiple IP addresses from the same devices, doing so perpetuates the illusion of a larger network than what exists. When connecting to each of the nodes depicted in the client UI below (several nodes reflecting one of three multi-homed devices RSA Research has identified) the exit IP addresses are randomly assigned from the large pool of available IP addresses.

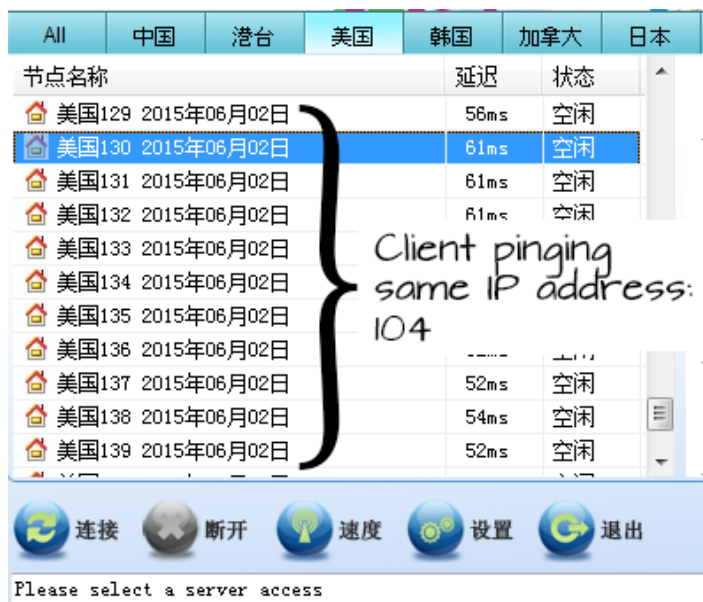


Figure 2. Screenshot of Terracotta client app, listing multi-homed nodes

- No public services other than PPTP VPN. In instances where RSA Research has confirmed the compromise of an organization, the victim organizations used their Internet-facing servers for various use cases, none of which included VPN or Windows Remote Access services. If these were compromised devices, we would expect the devices to be used by their legitimate owners for other purposes prior to being enlisted as Terracotta VPN nodes. If, on the other hand, a legitimate VPN provider was compromised, we expect the operators to have noticed that their authentication process and client-base had been hijacked.



Figure 3. RDP Login banner associated with possibly leased Terracotta VPN node

A login splash screen (Figure 3) associated with the device with hostname 3819027EEA6E42F indicates the use of Windows Server 2003 Enterprise x64 Server, with Simplified Chinese locale or Chinese language pack. The latter would be the Windows locale most-commonly used by mainland PRC or Singapore residents.

BEHIND TERRACOTTA NODES: THE VICTIMS

All of the compromised systems, confirmed through victim-communication by RSA Research, are Windows servers. RSA Research suspects that Terracotta is targeting vulnerable Windows servers because this platform includes VPN services that can be configured quickly (in a matter of seconds). While most of the Terracotta victims are smaller organizations without dedicated security staff, large organizations were not immune to exploitation by the Terracotta perpetrators. Organizations with confirmed compromised Windows servers include:

- Fortune 500 hotel chain
- A department of transportation in a U.S. state
- High tech manufacturer
- Fortune 500 engineering firm
- University in Taiwan
- University in Japan
- State university in the U.S.
- County government of a U.S. state
- Prize indemnity insurance company
- Microsoft Windows enterprise management application developer
- Boutique IT service provider
- Charter school
- Educational service provider
- Law firm
- U.S. university-affiliated company
- Web design and SEO consultant
- Physician's office
- Unified Communications as a Service (UCaaS) provider
- Business-to-Consumer (B2C) applications developer
- Public Convention center in a U.S. city
- Wireless test and measurement solutions provider
- IT Value Added Reseller (VAR) and services provider
- IT solutions provider/contractor for federal and local government organizations

The 23 organizations listed above represent at least 31 Windows server systems that were compromised and enlisted into Terracotta.

TERRACOTTA WINDOWS SERVER ENLISTMENT MODUS OPERANDI

A common trait shared with all confirmed victims is that they had Internet-exposed Windows servers without hardware firewalls. Additionally, for at least one victim with multiple servers exposed to the Internet, only those servers with the built-in Windows software firewall turned off were enlisted in the Terracotta VPN ecosystem. In one specific compromised system analyzed by RSA Research, the following sequence of events, shown in Figure 4, was noted prior to the system becoming a node in the Terracotta VPN ecosystem:

- 1 Brute force password attack on the "Administrator" user account, via DCOM Windows Management Interface (WMI) through TCP port 135. There are multiple security testing tools with this capability, including the popular CoreImpact python class `wmiexe.py`¹. The brute force activity was done from an IP address we call the "reconnaissance host" which was recently observed performing port 135 scanning on the Internet, according to DShield².
- 2 Remote connection using Administrator credentials from the reconnaissance host several hours later to disable the Windows Firewall and install the Telnet Service. Windows logs for this event sequence are consistent with those that would be recorded with use of standard remote administration tools available from Microsoft Management Console (MMC) via standard Windows Management Interface (WMI) protocols.
- 3 Login in via Remote Desktop (RDP) from a Windows system we call "base host", with hostname WEI-270FBC26C38, originating from IP ranges in the vicinity of Dongguan, a suburb of Guangzhou, China. This happens within minutes of events in sequence number two. RSA Research has obtained forensic images indicating that this hostname was used for compromises and enlistment from January 2014 to June 2015.

¹ <https://github.com/CoreSecurity/impacket/blob/master/examples/wmiexec.py>

² <http://dshield.org/ipdetails.html?ip=58.162.xx.xx>

- 4 From base host, uninstall Windows Defender and download and install custom Gh0st Remote Administration Tool (RAT) (dropper MD5: bccbba3ed45ead051f56fc62fef005a6) and/or custom Mitozhhan RAT (MD5: 7b18614df95e71032909beb25a7b1e87) and a Windows backdoor shell daemon listening on port 3422 (MD5: 531d30c8ee27d62e6fbe855299d0e7de).
- 5 Creation of new Windows account (actual examples include "mssql" and "krto") and addition of account to administrators group, from base host.
- 6 Days later, a login via RDP from base host in Dongguan, China using the account created in step five to install Network Policy and Access Services and Routing and Remote Access Services with custom remote access policy pointing at Terracotta Internet Authentication Services (IAS) servers.
- 7 Testing of Terracotta VPN centralized IAS authentication using "testwj" account from base host WEI-270FBC26C38.

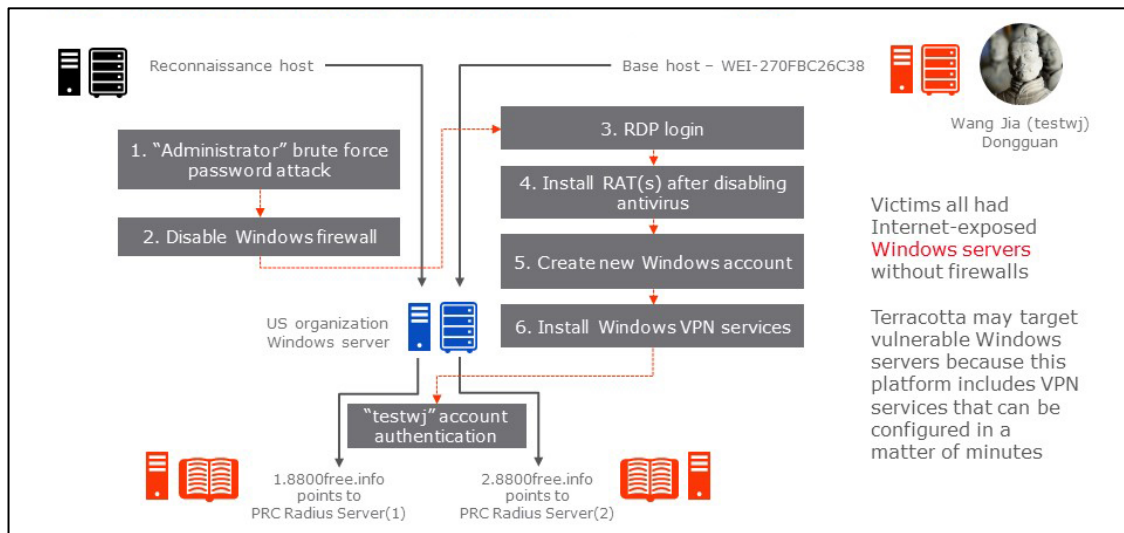


Figure 4. Terracotta VPN enlistment

THE ECONOMICS OF HACKING FOR A PROFIT

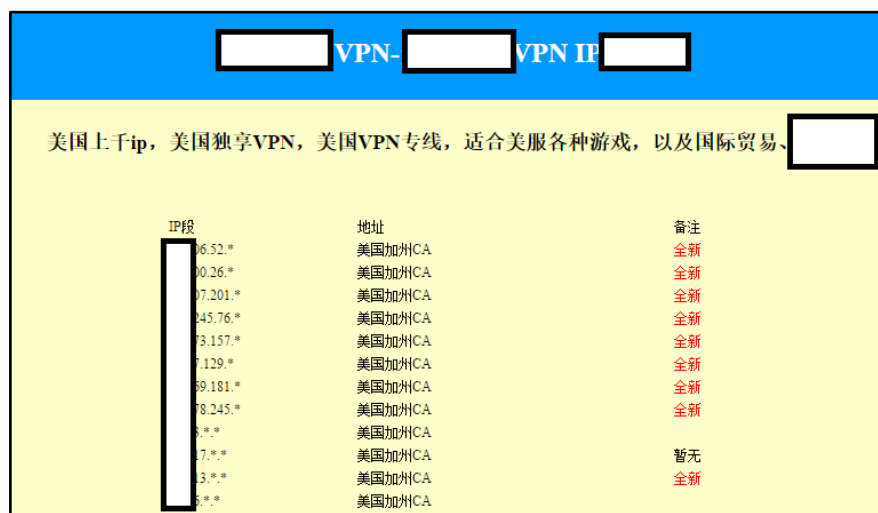
Why would a business need to hack servers for use in a VPN ecosystem, when Virtual Private Servers (VPS) are so readily and inexpensively available? Currently, high-quality VPS's with sufficient power for use as a VPN node can be leased for as little as \$5.00 per month in the U.S. However, VPN traffic is more bandwidth-intensive than CPU-intensive. Since many VPS solutions provide a base-level of bandwidth and charge for overage, the cost of bandwidth for a VPN service such as Terracotta would significantly affect operating expenses. Even if the monthly recurring bandwidth costs of using VPS servers were ignored, the logistics of managing the contracts and payments with foreign and domestic providers would add significantly to the cost of operations. Conservatively, RSA Research counted more than 300 different organizations behind the 1500+ nodes in the Terracotta VPN ecosystem.

Hypothetical Discussion: If the servers were legitimate, at least 300 monthly international transactions would be required to maintain the network. A more-profitable and simpler (if not legitimate) model may be to ensnare a seemingly endless supply of vulnerable servers on the Internet. RSA Research proposes that the Terracotta VPN provider "hacks and harvests" VPN nodes because this process is not only cheaper, but logistically easier than running a complex accounts payable operation required to maintain a global 1500+ node VPN ecosystem.

VPN NODES THAT DON'T "LOOK LIKE" VPN NODES

Several legitimate mainland PRC VPN providers were reviewed by RSA Research. These providers were consistent in that they ostensibly provided a list of all VPN IP addresses on their websites (Figure 5). A security analyst (or a content service provider with contractual restrictions on geographical distribution), would be able to enumerate hosts associated with the VPN provider and restrict accordingly.

In contrast, if a portion of your exit IP addresses appear to be associated with legitimate businesses and can't be easily classified as VPN nodes, then you may attract a customer interested in obscuring its origin. The Terracotta-branded providers do not publish such lists. Their exit nodes remain largely unrestricted, an apparent differentiator.



IP段	地址	备注
06.52.*	美国加州CA	全新
00.26.*	美国加州CA	全新
07.201.*	美国加州CA	全新
045.76.*	美国加州CA	全新
03.157.*	美国加州CA	全新
07.129.*	美国加州CA	全新
09.181.*	美国加州CA	全新
08.245.*	美国加州CA	全新
0.*	美国加州CA	
07.*	美国加州CA	暂无
03.*	美国加州CA	全新
05.*	美国加州CA	

Figure 5. U.S. Nodes as displayed on a legitimate VPN service website

WHO USES TERRACOTTA VPN?

To help characterize the Terracotta user base, RSA Research analyzed the Microsoft Remote Access Service (MSRAS) logs for a single Terracotta victim server for one month (Table 1).

Unique successfully authenticated connections	118,948
Unique client IP addresses	9,053
Client IP Addresses in mainland PRC	8,903 (98%)
Client IP addresses not in mainland PRC	150 (2%)
Unique client account names	723 (most connections used trial accounts)
Unique client host names	3,640

Table 1. Statistics from a month of logs on an enlisted Terracotta Node

Clearly, most users of Terracotta appear to originate within mainland PRC, as is consistent with where the service is marketed. In addition to the APT activity that has been observed, RSA Research believes that use cases include Great Firewall traversal, anonymity, peer to peer (P2P) file sharing and gaming acceleration; though this traffic analysis research is based on a limited number of network packet captures. Other (non-APT) criminal activity that may leverage Terracotta's anonymity is possible, but has not been observed to date. The clients of Terracotta may be entirely unaware of the organizations methods for obtaining servers and bandwidth.

SUSPECTED NATION STATE SPONSORED CAMPAIGNS LEVERAGING TERRACOTTA VPN

Since providing Terracotta VPN indicators to trusted partners, RSA Research has received several reports of suspected nation-state sponsored campaign activity originating from Terracotta VPN IP addresses. RSA Research can confirm that suspected nation-state actors have leveraged at least 52 Terracotta VPN nodes for exploitation of sensitive targets among Western government and commercial organizations. Perhaps one of the benefits of using Terracotta for Advanced Threat Actors is that their espionage-related network traffic can blend-in with 'otherwise-legitimate' VPN traffic.

TERRACOTTA VPN LEVERAGED FOR PHISHING AND ATTEMPTED EXPLOITATION OF A DEFENSE CONTRACTOR

RSA Research received a specific report from a large defense contractor concerning 27 different Terracotta VPN node IP addresses that were used to send phishing emails (Figure 6) targeting users in their organization. The phishing emails were simple HTML formatted emails with content pasted from legitimate online news articles. The HTML formatted emails were loaded with an intelligence-gathering tool known as a "web bug"³ that was specifically tailored to the recipient.

³ https://en.wikipedia.org/wiki/Web_bug

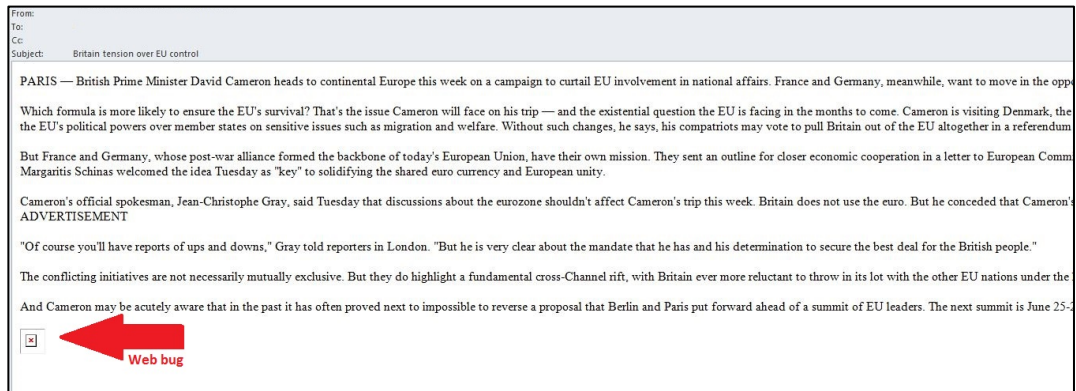


Figure 6. Redacted phishing email laden with web bug sent from Terracotta VPN node IP address

An image reference in the email pointed to a website controlled by the actors that spoofed a popular Webmail provider. The image reference appeared to have been crafted so as to entice the target into logging into the phishing website with their legitimate credentials (Figure 7), thereby sending the targets' webmail credentials directly to the malicious actors. Typically APT actors use the information they gather from web bugs and phishing to later perform highly targeted exploitation or intelligence collection on specific users who have met their criteria.

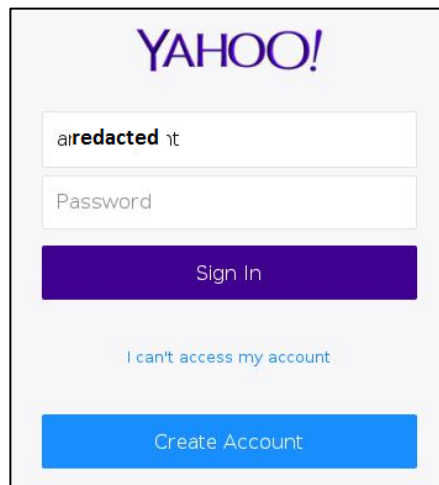


Figure 7. Spoofed login page for major webmail provider, linked from phishing email

RSA Research investigated the domain infrastructure related to the phishing activity described above and enumerated related domains, as shown partially redacted in Table 2.

The partial- and un-redacted domains below are representative of brands that are commonly spoofed for phishing purposes. All of these domains have been reported and are obvious spoofs. The domains we have redacted involve specific government and defense sector targets. These have been reported and the targets have been notified. Further details can be made available to industry partners.

Domains directly related to defense contractor phishing from Terracotta VPN nodes

weblogin-yahoo.com

weblogin-vxxxxxx.net

linkedinmember.com

auth-vxxxxxx.com

weblogin-live.com

[10 related domains based on common hosting]

Table 2. Terracotta-originating phishing campaign related domains

SHELL_CREW

As part of the investigation, RSA Research was able to track suspected Shell_Crew actors in their ongoing exploitation campaign of a sensitive network over several months. These actors connected to a Derusbi server variant "beachhead" on this target network.

Out of the thirteen different IP addresses used during this campaign against this one (APT) target, eleven (85%) were associated with Terracotta VPN nodes. At least in this month's long campaign, we see advanced threat actors using Terracotta VPN infrastructure to obscure their origins and cover their tracks.

For more information on these advanced threat actors, refer to the Shell_Crew report from the RSA Incident Response Team here: <http://www.emc.com/collateral/white-papers/h12756-wp-shell-crew.pdf>

TERRACOTTA VPN BREAKDOWN

A recent network node location breakdown of the Terracotta network indicates that a high percentage of nodes are in China, with secondary focus in the United States and South Korea. Additionally we see smaller quantities in other disparate locations.

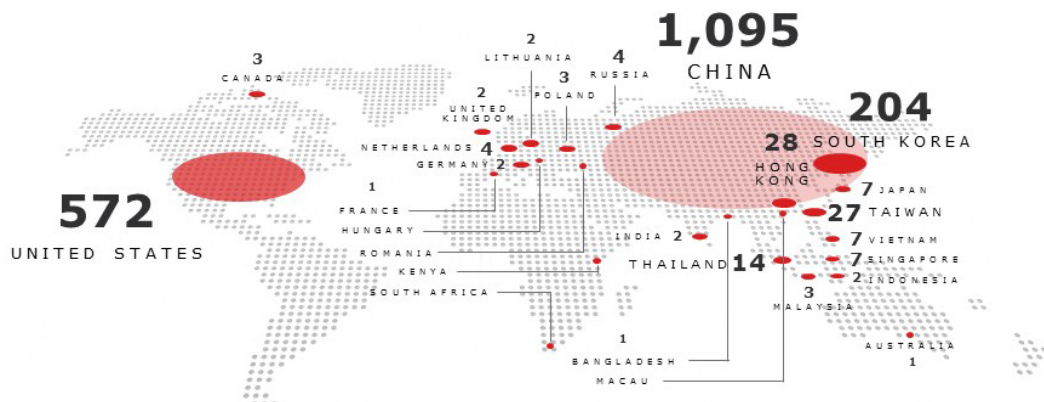


Figure 8. Geographic concentration of Terracotta VPN Nodes

DETECTION

Depending on what aspect of the attack you are looking for, detecting Terracotta VPN in your network will likely require a number of different detection methods and technologies.

DETECTING NODE ENLISTMENT ACTIVITY

If a host has been enlisted as a VPN node in the Terracotta network, the compromised server will beacon to the following URLs as the servers authenticate users to the VPN service:

- 1.8800free.info (currently resolves to IP address in Zhengzhou, Henan Province, PRC)
- 2.8800free.info (currently resolves to IP address in Hangzhou, Zhejiang Province, PRC)

Servers exhibiting this behavior should be examined for compromise.

DETECTING NODE USE IN ATTACKS

To detect the use of Terracotta VPN nodes in attacks, ingress/egress connections from the host nodes should be noted and investigated. Hits on these nodes would indicate anonymization activity from the Terracotta network.

DETECTING USE OF TERRACOTTA VPN RESOURCES

To detect users of this service, connections to “Client Authentication Domains” (Appendix 1) should be monitored. Hits to these domains would indicate an end-user using the downloadable VPN client to select VPN nodes for use. Additionally, hits to “Client Marketing Domains” (Appendix 1) may indicate an end-user “shopping” for access to the VPN service.

DETECTING TERRACOTTA ASSOCIATED MALWARE

RSA Research has associated several notable malware samples with the Terracotta eco-system. These binaries have been used to provide backdoor/RAT services on compromised servers. RSA Research has observed that this malware is commonly installed by the actors concurrently with other remote administration tools including Radmin, DameWare, and Windows telnet server. Other lateral reconnaissance and exploitation tools used by the Terracotta actors include various port scanners and password dumpers such as Mimikatz and a Chinese tool called DolphinQ.⁴ Additionally, many Terracotta nodes had sometimes multiple instances of CCProxy installed to provide additional anonymization services. These CCProxy instances used locally configured credentials, and not central authentication like the VPN services.

While this is not a thorough analysis of the malware encountered during this investigation, several samples were directly tied to the initial enlistment of the servers as nodes into the Terracotta VPN ecosystem, as mentioned in the Modus Operandi section.

Gh0st RAT MM523

File Size: 21.9 MB

MD5: bccbba3ed45ead051f56fc62fef005a6

C2: vpn.mm523.net:10000 (currently sinkholed by RSA Research⁵)

<http://www.trendmicro.com/vinfo/us/threat-encyclopedia/malware/zegost>

<http://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=TrojanDropper:Win32/Zegost.B#tab=2>

RSA Research refers to this variant, or build of Gh0st RAT as “MM523” based on the C2 domain. Gh0st is a full function Remote Administration Tool (RAT) with keystroke logger, file manager, remote terminal shell, screen control and capture, and many other functions. Pertinent analysis on Gh0st RAT is available⁶. Since the majority of confirmed Terracotta-compromised systems are running 64-bit Windows Server 2008 R2, this section will detail more findings that are pertinent to that platform, rarely covered by typical sandbox analysis.

This particular binary was found on only one system, but appears to be an installer or “dropper” for the Gh0st malware that was found on multiple Terracotta compromised servers prior to February 2015. This malware is unusually large because it is padded with zeros. The large file size may have been a rudimentary attempt to avoid antivirus or network security systems. To be sure, absent the padding, a binary comparison proves that the sample is identical to the sample submitted to VirusTotal in July 2014 with MD5 of e421d07c316ab6e04fd0bfa122f1d953.⁷

Gh0st was coded originally for Windows XP. Though the dropper will successfully install on more modern Windows systems, there are unresolved issues with its installation on Windows 7 and Windows Server 2008R2.

The dropper scans the Windows registry here:

```
HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Svchost\Netsvcs
```

It finds the first unused (stopped and disabled) service that runs under service process svchost netsvcs. On typical Terracotta victim servers, this has been the FastUserSwitchingCompatibility service, which is a deprecated service left-over from Windows XP for compatibility. Since FastUserSwitchingCompatibility it is not an actual service that can run on versions later than Windows

⁴ <https://www.virustotal.com/en/file/9b8257000b05116a3631630c44b9f6b18c13e5bc5635c1fa3f20a01f70380909/analysis/>

⁵ A sinkholed domain is one that was used by its owner specifically for malicious activity and thus subject to lawful seizure. Malware that is sinkholed is redirected to an analysis system controlled by researchers or law enforcement instead of the criminals. The sinkhole is then used for intelligence research and victim notification.

⁶ <http://www.mcafee.com/us/resources/white-papers/foundstone/wp-know-your-digital-enemy.pdf>

⁷ <https://www.virustotal.com/en/file/3a2d5ce9f5f953f0499773a05f26317f9f6745352031bb8dafbb6aadf0e8e57b/analysis/>

XP, Microsoft has omitted the service description text. So the Gh0st dropper scans to the next description, and artifacts arising from that issue include a misspelled and mismatched description for the hijacked FastUserSwitchingCompatibility which is "Windows Sxitscway Firewall/Internet Connection Sharing (ICS)". A Google search for the word "Sxitscway" will reveal other malware that encounters similar platform compatibility problems.

The dropper installs its service DLL named with five random letters with the following path in the normally hidden ProgramData directory. Example:

C:\ProgramData\Application Data\Storm\update\%SESSIONNAME%\hbeya.cc3

The Gh0st service DLL binary in this location is approximately 22MB in size, and because the file is generated dynamically, has a unique file hash for each installation.

Upon initial execution, the Gh0st RAT dropper is extremely busy, querying for some 75 URLs associated with legitimate antivirus vendors; however, no connections are made to these URL for C2. For control, the RAT connects to the IP found with a DNS query to vps.mm523.net on port 10000 using the same connection string as the "cb1st" variant of Gh0st analyzed by Norman in "The Many Faces of Gh0st" paper here:

<http://download01.norman.no/documents/ThemanyfacesofGh0stRat.pdf>

RSA Research determined that some 240 systems around the world are infected with this Trojan, including approximately 100 Terracotta VPN nodes.

Gh0st RAT GDS520

File Size: 204.5KB

MD5: possibly 81c08ae40700d863f5dbd35599192962 and/or ef938cd1594b6b44507c6423cd39d5f5

C2: gds520.com:8086 (Active)

Following the neutralization of the MM523 Gh0st RAT communication with the RSA Research seizure of its C2 domain, RSA Research observed malicious services installed by a dropper variant very similar to the MM523 Gh0st variant on newly compromised Terracotta victims. While similar to the "Gh0st RAT MM523" build, this build we dub GDS520 has a different service DLL location and C2 URL. The GDS520 sample had been in the wild before the RSA Research sinkholing of mm523.net, based on the date two dropper variants were uploaded to VirusTotal. Similar to Gh0st RAT MM523, these variants are characterized by DNS lookups to multiple antivirus vendor update URLs, in addition to the C2 URL, gds520.com over port TCP port 8086. The Ghost RAT GDS520 service DLL is named with five random letters and is installed in the following location with the example file name:

C:\ProgramData\DRM\%SESSIONNAME%\vxujx.cc3

Notably, the dropper deletes itself after successfully installing the RAT service. This is unlike the Gh0st RAT MM523 variant, which did not delete itself. Finally, the two GDS520 Ghost RAT variants found on VirusTotal were built with file properties to resemble a legitimate Microsoft program (Figure 9), and included a digital certificate as one of the executable's resources, which can be displayed in the file properties digital signatures tab (Figure 10). RAT files were appended with a digital signature taken from a legitimate file signed by Kaspersky Lab. Since the signature corresponds to a different file, it appeared as invalid. Any more than cursory review of the dropper executable properties would reveal the invalid signature. These dropper samples used the exact same Kaspersky certificate described in the article "Certificate Snatching—Zeus Copies Kaspersky's Digital Signature" by TrendMicro.⁸

⁸ <http://blog.trendmicro.com/trendlabs-security-intelligence/certificate-snatching-zeus-copies-kasperskys-digital-signature/>

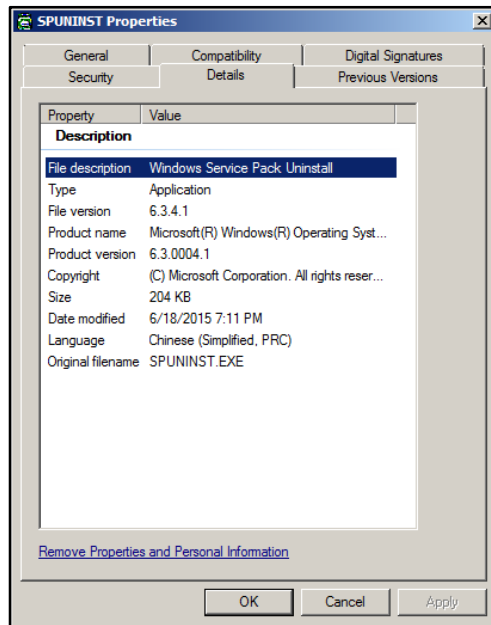


Figure 9. Gds520 Gh0st RAT installer file details

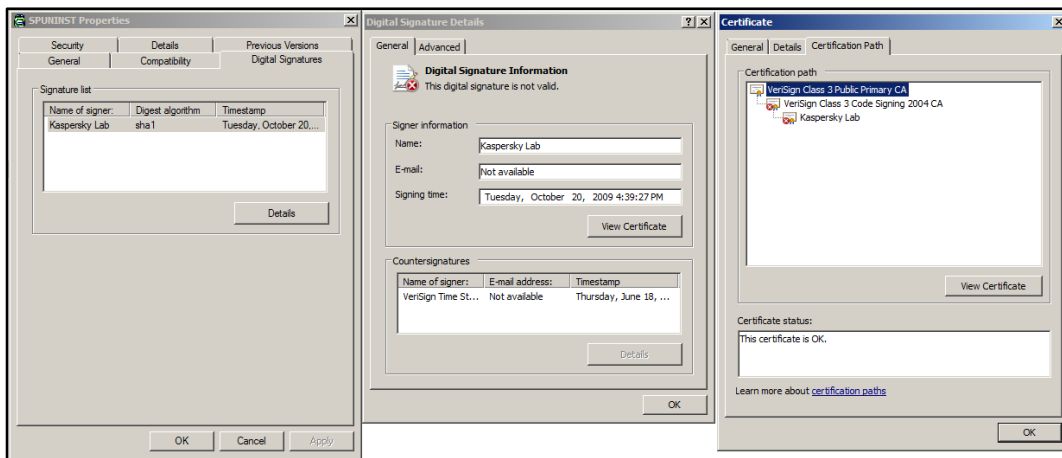


Figure 10. Gds520 Gh0st RAT installer with invalid code signing using Kaspersky public certificate

On one compromised system investigated in May of 2015, forensic artifacts showed the source IP address of the GDS520 installer (Figure 11).

```

http://211.153. :7788/
application/x-msdownload
\Users\Administrator\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5\AZMTSYQM\s[1].exe
http://211.153. :7788/s.exe
\Users\Administrator\Desktop\s.exe

```

Figure 11. Forensic artifacts left behind on a victim server by the actor downloading the GDS520 Gh0st RAT installer from a Beijing IP address

A cache of the page indicated it was from a type of ephemeral file server known as HTTPFileServer (HFS)⁹. The HFS server cached page showed that the HFS daemon had been up for 4 minutes (Figure 12). Fortunately for the investigation, the ephemeral HFS daemon maintains usage statistics. Out of the 37 files available on the HFS page to the Terracotta actor, the GDS520 Gh0st RAT appeared to be the most commonly downloaded, with 1225 total downloads (Figure 12).

⁹ <http://www.rejetto.com/hfs/>

0 folders, 37 files - Total: 174.11 MB			
Filename	Filesize	Filetime	Hits
360jix.zip	22.90 MB	11/22/2014 17:32	2
445.zip	6.02 MB	5/14/2014 18:38	39
7z920.exe	1.06 MB	11/23/2014 12:03	94
BaiduYunGuanjia_5.2.1_setup.1426820724.exe	10.94 MB	4/1/2015 18:25	21
bp.exe	204.48 KB	2/7/2014 12:15	281
btc32.zip	2.80 MB	12/11/2014 20:38	61
btc64.zip	3.79 MB	3/18/2015 12:06	340
CrystalMinesSetup1.0.2.81.exe	5.02 MB	4/11/2015 23:15	17
dubroute_2.1.rar	3.72 MB	1/29/2015 17:39	79
hex.hta	1.77 KB	1/15/2015 23:45	3
hfs.exe	559.50 KB	11/22/2014 21:12	44
HM.exe	298.86 KB	4/24/2015 19:13	23
HM.zip	105.60 KB	4/24/2015 19:14	63
HS-1433.zip	1.41 MB	4/8/2015 13:25	35
IISPutScanner.exe	490.50 KB	12/26/2014 17:35	31
inst.exe	1.48 MB	12/5/2014 21:55	45
k8team123.exe	40.00 KB	12/22/2014 15:01	26
lcx.exe	39.52 KB	12/5/2014 22:44	29
mafix.tar.gz	436.24 KB	12/2/2014 22:31	1
MZD.exe	54.50 KB	12/5/2014 14:34	63
net1.exe	139.00 KB	1/3/2015 13:39	4
NT_scan.zip	73.27 KB	4/15/2014 10:52	78
PEERInstall.exe	99.39 MB	1/15/2015 22:00	5
putty.exe	654.50 KB	12/13/2014 18:59	6
ReadPWD.exe	64.00 KB	12/5/2014 14:35	323
ReadPWD86.exe	92.00 KB	10/17/2012 1:24	117
s.exe	204.48 KB	12/5/2014 14:12	1225
struts2-vul-fix.rar	13.73 KB	4/10/2014 9:22	22
Sunos.exe	2.54 MB	4/24/2015 19:06	14
svchost.exe	204.48 KB	12/15/2014 22:39	758
Utilman.exe	3.45 MB	9/30/2014 11:34	48
vc2008.zip	4.26 MB	11/22/2014 20:49	1
vpn.txt	2.05 KB	10/8/2014 19:23	195
Win32.exe	47.00 KB	12/12/2014 21:11	147
Win64.exe	85.50 KB	4/14/2015 18:17	433
获取哈希值_11775.rar	367.06 KB	2/8/2015 15:46	3
智障arp.zip	1.25 MB	12/18/2014 19:28	8
HttpFileServer 2.2f			
Srvertime: 2015-5-3 8:27:43			
Uptime: 00:04:03			
Build-time: 0.047			

Figure 12. HFS-hosted tool repository from which Terracotta actor downloaded the GDS520 RAT installed on victim server. Note the yellow-highlighted information for “s.exe”.

The HFS daemon was running on an IP address from a range assigned to a middle school in Beijing according to Whois information¹⁰. Virus Total^{11 12 13 14} reveals that hosts in this IP range have been used, extensively in the first half of 2015, to host malicious tools including the GDS520 Gh0st RAT variant and other exploitation tools found on at least three Terracotta victim systems. Also notable in Figure 12 is the third most-often downloaded tool from the actor's HFS page, named "Win64.exe"¹⁵. RSA Research found this on one Terracotta victim server, and determined this to be a variant of the Windows privilege escalation exploit tool as described by CrowdStrike in a blog post on Hurricane Panda¹⁶. RSA Research does not know if the Beijing IP address range was leveraged exclusively by Terracotta operators.

Mitozhan Trojan

File Size: 87 KB

MD5: 7b18614df95e71032909beb25a7b1e87

C2: vps.mm523.net:81 (sinkholed)

This malware copies itself to the Windows directory (C:\Windows) and gives itself a new random name. Every time the malware runs, the executable name will vary but the file name length remains the same; 6 characters.

Example:

C:\WINDOWS\fatjse.exe

The Image Path of the newly-copied file is then used to add a new service to the ControlSet Registry Key. This will ensure persistence on the infected machine. The name of the new service (GHIJKL NOPQRSTU WXY) might be suspicious to administrators.

Example:

RegKey Name: MACHINE\SYSTEM\CONTROLSET001\SERVICES\GHIJKL NOPQRSTU WXY

RegKey Data: C:\WINDOWS\fatjse.exes\0

The malware performs a DNS request to vps.xxxxx.net for resolution of its controller. The infected machine connects to the controller over TCP port 81 with the following initial connection string (Figure 13).



Figure 13. Mitozhan C2 connection string

Two strings of interest are revealed upon examination of the process in memory.

%c%c%c%c%c%c%c.exe

GET %s HTTP/1.1Content-Type: text/htmlHost: %sAccept: text/html, */*User-Agent:Mozilla/4.0 (compatible; MSIE %d.00; Windows NT %d.0; MyIE 3.01)

Search engine results for the last part of the UA string MyIE 3.01 show the exact UA string mentioned in a blog post by FireEye in 2010¹⁷. The FireEye blog references another blog by researchers from Arbor Networks¹⁸. The latter blog describes in more

¹⁰ <https://whois.domaintools.com/211.153.xx.x>

¹¹ <https://www.virustotal.com/en/ip-address/211.153.xx.x/information/>

¹² <https://www.virustotal.com/en/ip-address/211.153.xx.x/information/>

¹³ <https://www.virustotal.com/en/ip-address/211.153.xx.x/information/>

¹⁴ <https://www.virustotal.com/en/ip-address/211.153.xx.2xx/information/>

¹⁵ <https://www.virustotal.com/en/file/d7bd289e6cee228eb46a1be1fcdc3a2bd5251bc1eafb59f8111756777d8f373d/analysis/1429772817/>

¹⁶ <http://blog.crowdstrike.com/crowdstrike-discovers-use-64-bit-zero-day-privilege-escalation-exploit-cve-2014-4113-hurricane-panda/>

¹⁷ <https://www.fireeye.com/blog/threat-research/2010/10/avzhan-botnet-the-story-of-evolution.html>

¹⁸ <http://www.arbornetworks.com/asert/2010/09/another-family-of-ddos-bots-avzhan>

depth the malware behavior, which shares several elements with the sample under investigation, including the use of a raw TCP connection to the server, the UA string in memory, and the pattern to generate the executable name.

The legitimate properties and text depicted in the file appear to obscure the actual malicious intent. The file is named after a very popular photo markup program in China called 美图秀秀¹⁹ or "Mito Xiu Xiu" (Figure 14).

Property	Value
Description	
File description	美图秀秀
Type	Application
File version	1.0.0.1
Product name	美图秀秀 应用程序
Product version	1.3.0.1
Copyright	版权所有 (C) 2013
Size	87.3 KB
Date modified	1/11/2014 11:14 PM
Language	Chinese (Simplified, China)
Original filename	美图秀秀.EXE

Figure 14. Mitozhan file properties shares name and description with popular benign program

RSA Research determined that approximately 180 systems were infected with this Trojan, approximately one third of which were active in the Terracotta VPN node ecosystem.

Backdoor Liudoor

File Size: 87 KB

MD5: 531d30c8ee27d62e6fbe855299d0e7de²⁰

C2: 0.0.0.0:3433

This is a simple backdoor similar to the common Portless Backdoor²¹ found running as a service on at least five Terracotta VPN victim servers, that RSA Research has dubbed Liudoor. It was installed as Windows\SysWOW64\rasauto.dll running as what would be the unused "RasAuto" service on victim Windows Server 2008 R2 systems.

While RSA Research did not find the dropper for this backdoor, it could have just as easily been installed with a batch script. This sample binds to TCP port 3433 and waits for an incoming request, probably from a dedicated client used by its operator. It will send the 4 bytes "pass", it expects to receive the binary string "E10ADC3949BA59ABBE56E057F20F883E" (shown here in ASCII text). This is the MD5 hash of the ASCII string "123456". The backdoor process will compare what is passed from the client to that hard coded value, and if successful it will send back "succ", if not it will send back "fail".

Once the sample has successfully authenticated it will create a thread and pipe data back and forth to the Windows command shell process, cmd.exe. It takes the input and parses the string sent to the sample for 0x0D (the obfuscation XOR key) or carriage return...and then passes everything before that to cmd.exe. The shell can be halted with the "exit" command. Other hard coded binary options include a certain value that will run the console program "nbstat.exe" for NetBIOS network information, which might be useful to its operator for lateral exploitation of other Windows computers on the victim network. RSA Research found similar Backdoor Liudoor files on VirusTotal with the following characteristics:

78b56bc3edbee3a425c96738760ee40622 listens on port 3340

5aa0510f6f1b0e48f0303b9a4bfc641e23 listens on port 3433

2be2ac65fd97ccc97027184f0310f2f324 listens on port 1234

On more recently discovered Terracotta victims, Liudoor was observed to listen on TCP port 64111 or 33911.

¹⁹ <http://xiuxiu.web.meitu.com>

²⁰ <https://www.virustotal.com/en/file/ad1a507709c75fe93708ce9ca1227c5fefa812997ed9104ff9adfec62a3ec2bb/analysis/>

²¹ http://www.symantec.com/security_response/writeup.jsp?docid=2003-122516-0717-99&tabid=2

²² <https://www.virustotal.com/en/file/deed6e2a31349253143d4069613905e1dfc3ad4589f6987388de13e33ac187fc/analysis/>

²³ <https://www.virustotal.com/en/file/4575e7fc8f156d1d499aab5064a4832953cd43795574b4c7b9165cdc92993ce5/analysis/>

²⁴ <https://www.virustotal.com/en/file/e42b8385e1aec889a94a740a2c7cd5ef157b091fabd52cd6f86e47534ca2863e/analysis/>

DETECTING TERRACOTTA ACTIVITY IN RSA SECURITY ANALYTICS AND RSA ECAT

Organizations with robust and consistently applied security controls on Internet-facing infrastructure should face little risk that their servers would be enlisted as VPN nodes by Terracotta actors. Two Fortune 500 companies that were identified as victims were exceptions as the comprehensive application of security controls fell short. More threatening to otherwise well-defended organizations is the threat of advanced threat actors originating from legitimate, but compromised, organizations. Any network connection with a Terracotta VPN node should be treated with great suspicion and investigated immediately. Built into RSA Security Analytics is the automatic threat intelligence aggregation and delivery system known as RSA Live. Updated Terracotta node IP addresses are provided in RSA Live as part of the suspect VPN node feed, and available upon request. In Figure 15, RSA Security Analytics has alerted on the Derusbi server handshake parser from RSA Live. It also has alerted on the source of the malicious Derusbi Command and Control (C2) which is a Terracotta node, described as a criminal VPN service exit node by Security Analytics.

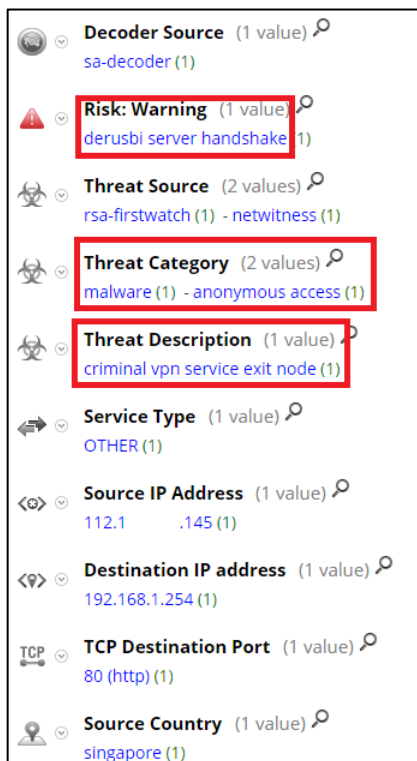


Figure 15. RSA Security Analytics detects advanced threat control of Derusbi server backdoor originating from Terracotta VPN Node

In Figure 16, a redacted screenshot from RSA Security Analytics shows an alert on a suspicious login to an otherwise secure website from a Terracotta VPN node. Any authentication from Terracotta to an organization's secure websites should be treated as hostile and investigated accordingly.



Figure 16. RSA Security Analytics detection of secure website login (redacted) from Terracotta VPN

DETECTING TERRACOTTA MALWARE USING RSA SECURITY ANALYTICS AND ECAT

“An ounce of prevention is worth a pound of cure.” Certainly this idiom from Ben Franklin applies to efforts to defend against this class of threats (not particularly sophisticated, opportunistic, but potentially very costly). RSA Research assesses that had the Windows firewall been turned on, and the default “Administrator” account been renamed in each of the victim systems examined, the systems would not have been compromised with the methods employed by Terracotta. Still, in both large and small organizations, a dichotomy may manifest between a “Security 101” policy and application of that policy, especially in development and cloud environments.

Note: This is not intended to be a cyber-hunter’s cookbook for finding Terracotta activity with RSA Security Analytics and ECAT, but rather to offer takeaways on the indicators quickly identified by these tools. The “out of the box” Gh0st protocol parser from RSA Live detects the “cb1st” Gh0st protocol string used by both the GDS520 and MM523Gh0st RAT variants, highlighted in red in Figure 17. Security Analytics shows an actual victim system in Iran that was infected with the now-neutralized MM523 Gh0st RAT variant calling-back to a RSA Research sinkhole.

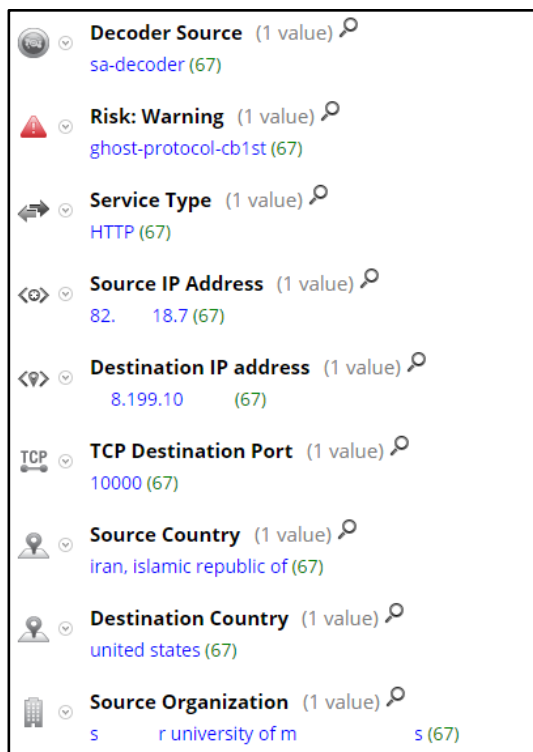


Figure 17. Gh0st protocol employed by MM523 Gh0st RAT detected by RSA Security Analytics

RSA ECAT will readily detect both Gh0st RAT variants employed by the Terracotta actors. In Figure 18, RSA ECAT has raised the Threat Level scores from low single-digit numbers to well above 100 when the GDS520 Gh0st RAT was installed.

Machine Status	Machine Name	Threat Level	Score	ECAT Version	Last Scan	Username	Online
	DEVAPP2		175	4.0.0.3	6/18/2015 9:33:06 PM	Administrator	<input checked="" type="checkbox"/>
	DEVWKST018		143	4.0.0.3	6/18/2015 2:05:50 AM	IEUser	<input checked="" type="checkbox"/>

Figure 18. Raised threat level scores indicate malware infection on server and workstation

Double clicking on the workstation in the RSA ECAT console will bring up details about the system, where an analyst can drill-down into the network connections, and responsible processes. In Figure 19, a Security Operations Center (SOC) analyst would be alerted by (illustrated in red boxes) the high score, the Suspicious Threads, and then hone in on the Gh0st C2 connections identified by RSA ECAT.

DEVWKST018

Admin Status: Score: **407**

Last Seen: 6/19/2015 5:16:09 PM

Comment:

Show Whitelisted
Hide Good Files
Hide Valid Signature

Category	Items	Sus...	Process	Module	IP	Domain	Port	Protocol
Live			svchost.exe	svchost.exe	::		50396	Tcp
Processes	38	28	wininit.exe	wininit.exe	::		49152	Tcp
DLLs	3	2	ntkrnlpa.exe	ntkrnlpa.exe	::		445	Tcp
Drivers	149	111	services.exe	services.exe	::		49155	Tcp
Inventory			lsass.exe	lsass.exe	::		49158	Tcp
Autoruns	4	4	svchost.exe	svchost.exe	::		49156	Tcp
Services	402	241	svchost.exe	svchost.exe	::		49153	Tcp
Tasks	31	31	svchost.exe	svchost.exe	::		3389	Tcp
Hosts	0	0	svchost.exe	svchost.exe	::		135	Tcp
Files	842	267	svchost.exe	svchost.exe	239.255.255....		3702	Udp
Anomaly			svchost.exe	svchost.exe	224.0.0.252		5355	Udp
Image Hooks	0	0	Autoruns.exe	Autoruns.exe	213.198.96.66	ctldl.windowsupdate.com	80	Tcp
Kernel Hooks	0	0	svchost.exe	svchost.exe	210.127.1...	gds520.com	8086	Tcp
Windows Hooks	0	0	svchost.exe	svchost.exe	210.127.1...	gds520.com	8086	Tcp
Suspicious Threads	1	1	EcatService.exe	EcatService.exe	192.168.88.244		444	Udp
Registry Discrepancies	0	0	EcatService.exe	EcatService.exe	192.168.88.244		443	Tcp
History			MpCmdRun.exe	MpCmdRun.exe	191.237.208....	spynet2.microsoft.com	443	Tcp
Network	37	37	svchost.exe	svchost.exe	184.86.40.154	www.microsoft.com	80	Tcp
Tracking	215	169						

2 items selected (37 total)

Figure 19. Suspicious network connections to the Gh0st C2 Domain as seen in RSA ECAT console

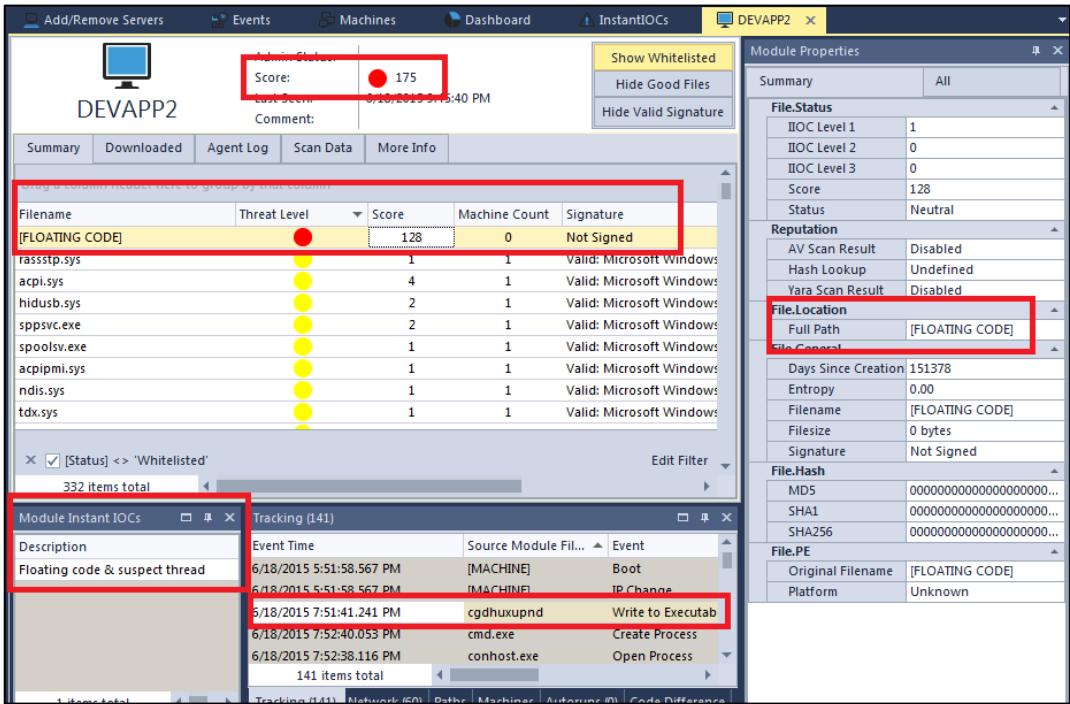


Figure 20. RSA ECAT uses IIOCs to identify floating code employed by Gh0st RAT malware

In our Gh0st RAT malware scenario, the SOC analyst would be able to identify the infections of a server and workstation in RSA Security Analytics. The red boxes in Figure 20 illustrate Gh0st RAT protocol detection and botnet threat categorization by RSA Security Analytics. An analyst also might notice the unusual communications port.

Decoder Source (1 value) 🔍
sa-decoder (749)

Risk: Warning (1 value) 🔍
ghost-protocol-cb1st (749)

Threat Source (1 value) 🔍
netwitness (281)

Threat Category (1 value) 🔍
botnet (281)

Service Type (1 value) 🔍
OTHER (749)

Source IP Address (2 values) 🔍
10.152.152.55 (513) - 10.152.152.65 (236)

Destination IP address (1 value) 🔍
210.127. (749)

TCP Destination Port (1 value) 🔍
8086 (749)

Destination Country (1 value) 🔍
korea, republic of (749)

Destination Organization (1 value) 🔍
s .ro (749)

Figure 21. RSA Security Analytics alerts on system infected with Gh0st RAT as it calls back to C2 IP address on port 8086

While the particular variant of the Mitozhan Trojan described in this paper’s malware analysis section has been neutralized by RSA Research with the seizure of its C2 domain; it is likely that other variants with different C2 domains persist. RSA developed a Lua parser to detect Mitozhan Command and Control (C2) activity, now available through RSA Live and included as an appendix. Figure 22 is a redacted screenshot showing the Mitozhan Lua parser in action as it alerts on Mitozhan C2 activity on a RSA Research sinkhole.

The screenshot displays a list of fields from a security analytics tool, each with a search icon. The 'Alerts' field is highlighted with a red box and contains the value 'mitozhan'. Other fields include 'Decoder Source' (sa-decoder), 'Service Type' (HTTP), 'Source IP Address' (12. .163), 'Destination IP address' (19 .129), 'TCP Destination Port' (81), 'Source Country' (united states), 'Destination Country' (united states), and 'Source Organization' (at&t services).

Field	Value
Decoder Source	sa-decoder (2)
Alerts	mitozhan (2)
Service Type	HTTP (2)
Source IP Address	12. .163 (2)
Destination IP address	19 .129 (2)
TCP Destination Port	81 (2)
Source Country	united states (2)
Destination Country	united states (2)
Source Organization	at&t services (2)

Figure 22. LUA Parser used to detect the Mitozhan C2 Activity in RSA Security Analytics

Mitozhan Trojan is also readily detected upon initial scan with RSA ECAT. Figure 23 shows the initial RSA ECAT console display for the infected system, with initial indicators marked in red boxes.

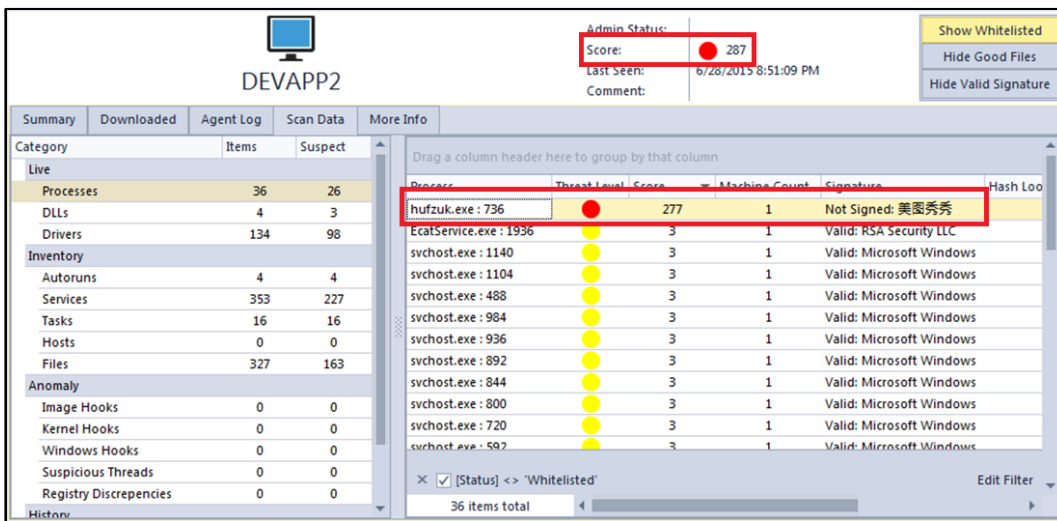


Figure 23. RSA ECAT console shows infection with Mitozhan. Note the high threat score, file name with random letters, and the unsigned executable with Chinese name

While RSA ECAT can detect a never-before-seen malware infection out-of-the-box without signatures, a well-prepared SOC will have signatures to help identify the threats behind the malware. That is where the built-in Yara features of RSA ECAT really shine. Yara is an open source tool that helps threat intelligence analysts and malware researchers classify and identify malware with granularity that no antivirus product can match. Using the Yara signature included in the Appendix, our example SOC analyst homes in on a suspicious rasauto.dll process identified by RSA ECAT as unsigned in Figure 24. By right-clicking on the suspicious process, the analyst can initiate a Yara scan using pre-configured rules

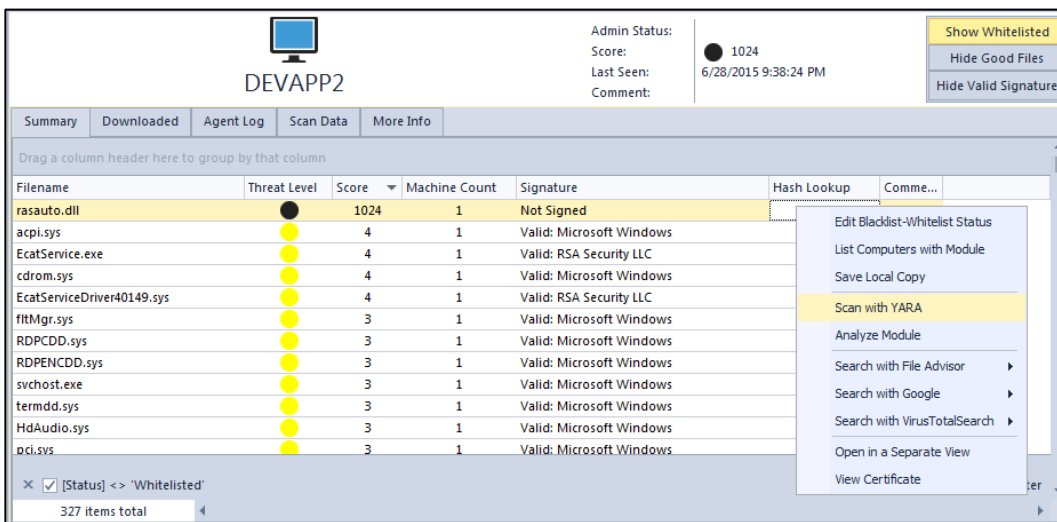


Figure 24. ECAT's YARA integration allows the SOC analyst or incident responder to quickly identify malware that may be associated with a specific threat

In this scenario, the SOC analyst has used ECAT to scan the suspicious process. As illustrated with the red box on the right of Figure 25, the Yara result is a confirmed infection with Liudoor. The Liudoor YARA signature is included in the Appendix

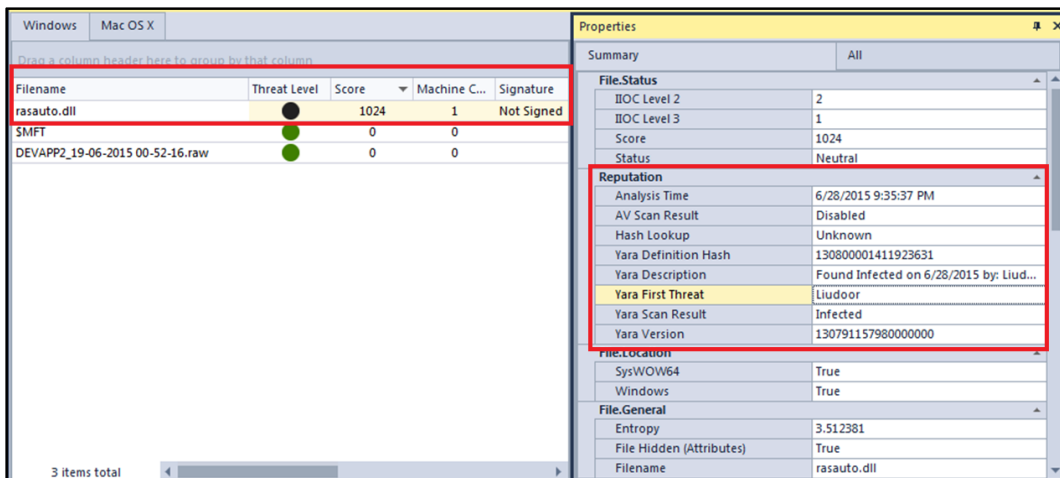


Figure 25. RSA ECAT indicates the YARA scan results. Backdoor Liudoor found!

For more technical details on how RSA ECAT can be used to proactively detect malware not discovered by traditional methods including antivirus, refer to the whitepaper RSA Incident Response: An APT Case Study.

<https://blogs.rsa.com/wp-content/uploads/2015/05/RSA-IR-Case-Study.pdf>

Terracotta Indicators for Security Analytics have been loaded into the following feeds in RSA Live:

- RSA Firstwatch APT Threat Domains**
- RSA Firstwatch Command and Control Domains**
- RSA Firstwatch Criminal VPN Exit IPs**
- RSA Firstwatch Insider Threat Domains**

PREVENTION

Terracotta VPN operators are not using sophisticated methods to harvest their VPN nodes from vulnerable organizations around the world. RSA Research assesses that any one of the following hardening steps would have prevented each of the confirmed victim compromises:

- 1 Block port 135 on external router and/or firewall
 - a. There is no known business-use for having port 135 exposed to the Internet
 - b. Recommend: hardware firewall configured with “allow inbound by exception” policy
- 2 Rename “Administrator” account on all Windows systems to a unique alphanumeric name
- 3 Use a strong (bi-case letters, numbers plus multiple special characters) 15 character+ password that does not use keyboard patterns
 - a. Keyboard patterns are found in nearly all password cracking dictionaries
 - b. Recommend: regularly change passwords

In contrast to the simple security controls that can prevent enlistment of an enterprise’s Windows servers into the Terracotta VPN node ecosystem, detecting advanced threat actors who are using Terracotta VPN nodes to hide their origin is more complicated. Infallible prevention may not be possible, and therefore detection is key. Use non-signature-based network analysis and end-point analysis capabilities such as provided by RSA Security Analytics and RSA ECAT to proactively detect and thwart compromise of your organization’s network, before your most valuable asset---your information— is compromised.

ATTRIBUTION AND PATTERN OF LIFE

Terracotta is a PRC-based operation that uses opportunistic, large-scale exploitation methods to obtain and augment a global, highly-marketable VPN service. RSA Research has no evidence suggesting that advanced threat actors such as Shell_Crew, or other suspected nation-state sponsored threat actor group is involved in any of the Terracotta exploitation activities. The attractiveness of the Terracotta ecosystem to advanced threat actors may be strictly utilitarian: a very low-cost platform for attacks that serves to ultimately reduce the probability of detection.

All compromised systems investigated by RSA Research were enlisted by actors originating primarily from IP ranges in Dongguan and other areas of the Guangzhou megalopolis, or from the city of Wuhan. The Terracotta exploitation activity from Dongguan took place primarily during weekends and hours outside of the normal mainland PRC workday using the following Windows hostname:

WEI-270FBC26C38

Forensic images reveal this hostname was consistently used in initial victim compromise from late 2013 through June 2015.

Exploitation activity originating from Wuhan took place during normal PRC work week days and hours. The following hostname was used:

QT-201312081446

In Terracotta system compromises investigated in 2015, there appeared to be coordination between the actor(s) originating from Dongguan IP addresses, and the actor(s) originating from Wuhan IP addresses. In six out of seven systems examined, the initial VPN test connection on a newly compromised server originated from Windows hostname WEI-270FBC26C38 with Dongguan IP address, which was shortly followed by a VPN test connection using the Windows hostname QT-201312081446 from a Wuhan IP address. Only after the successful connection from Wuhan was completed, did the node appear to be added to the Terracotta node list displayed by Terracotta brand software clients.

CONCLUSIONS

The Terracotta VPN system is marked by a grey-market anonymization ecosystem that is constructed, at least partially, of hacked servers. The Terracotta node ecosystem appears to enable better anonymity for advanced threat actors than would otherwise be allowed by a more conventional VPN service with a legitimate and transparent node infrastructure.

APPENDIX

Malware Sample Hashes

Malware Domains

Yara Signatures

C2 Lua Parsers

Terracotta User Account Authentication URLs

AVAILABLE TO INDUSTRY PARTNERS UPON REQUEST

Terracotta VPN Client Marketing Website Domains

Terracotta Software Client Authentication Domains

Current Terracotta Node List

Email conops@rsa.com for more information.

AUTHORS

Kent Backman, Primary Research

Alex Cox, Contributing

Steven Sipes, Contributing

Ahmed Sonbol, Contributing

RSA Incident Response Team, Contributing

RSA Labs, Contributing

The authors would like to thank a number of colleagues from RSA and industry for their advice and assistance on this project.