JUNE 2017

In the Boxing Ring

Network Box Technical News

from Mark Webb-Johnson, CTO Network Box

Welcome to the June 2017 edition of In the Boxing Ring

This month, we discuss **How to Survive a Trojan/Ransomware attack,** which compromises your workstation/server so that it can be used by a remote attacker. Ransomware is one form of trojan that encrypts files on a compromised system and demands payment to decrypt. On pages 2 to 4, we discuss this in greater detail, and outline best practices to mitigate against these threats.

Recently, the US-CERT and Department of Homeland Security released a National Cyber Awareness System alert: **TA17-156A**, regarding **SNMP (Simple Network Management Protocol) Abuse**; which can be used to gain authorized access to network devices. On page 5 we discuss this in further detail, along with prevention and mitigation recommendations.

On page 6, we highlight the features and fixes to be released in this month's patch Tuesday for Network Box 5.

Finally, in light of the recent WannaCry Ransomware outbreak, Network Box Managing Director, Michael Gazeley, was interviewed by various media outlets, and on page 7 we highlight some of the media coverage. In addition, Network Box Hong Kong participated in the SCMP 5th Redefining Hong Kong debate series, and Network Box Australasia was at the CERT NZ Launch event.

Mark Webb-Johnson
CTO, Network Box Corporation Ltd.
June 2017

You can contact us here at HQ by email (nbhq@network-box.com), or drop by our office next time you are in town. You can also keep in touch with us by several social networks:

twitter http://twitter.com/networkbox

facebook http://www.facebook.com/networkbox
http://www.facebook.com/networkboxresponse

LinkedIn http://www.linkedin.com/company/network-box-corporation-limited

Google+ https://plus.google.com/u/0/107446804085109324633/posts

In this month's issue:

NETWORK BOX

How to be a PREPPER

(aka How to Survive a Trojan/Ransomware attack)

Back in May 2013, we published the first of our "How to be a Prepper" articles, concerning surviving a DDoS attack. This month, we'll like to follow up with more preparedness, by showing you how to survive a Trojan/Ransomware attack.

Trojan/Ransomware: Malware that gets onto a workstation/server in order to compromise that computer so that it can be used by a remote attacker. Ransomware is one form of trojan that encrypts files on the target computer and demands payment to decrypt.

Preppers: Survivalists. Individuals or groups who are actively preparing for emergencies.

NETWORK BOX

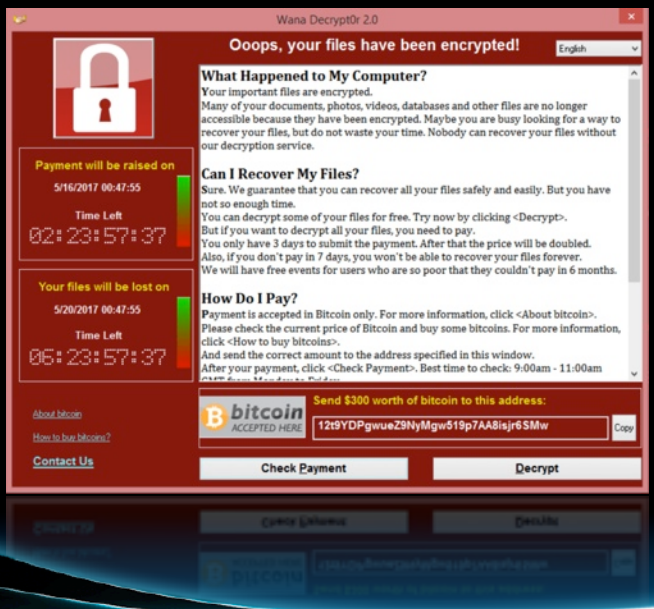
Scope

Of the 11+ million anti-malware signatures that Network Box 5 employs, approximately half are for Trojans - making these the #1 prevalent form of malware that Network Box protects against. While there are often thousands of variants of a particular trojan, we're still tracking almost 12,000 different families of trojans (including heuristic, non-signature based, protection for almost 5,000 of those). We classify close to 5% of the trojans we see as Ransomware.

Source of the Attack

The vast majority of trojans get into your network via trojan dropper/downloader malware. This special class of malware often include dozens of different exploits for known vulnerabilities in email browsers, mail clients, plugins, applications, and operating systems. The dropper/downloader generally come in as attachments to eMail messages, or website downloads. Once executed, the dropper/downloader usually uses the HTTP or HTTPS protocol to download the trojan payload itself, and install it onto the target computer.

The recent Wannacry Ransomware was unusual in that it primarily used a network-level exploit of a Microsoft SMB v1 vulnerability, and propagated as a network worm (it could propogate horizontally across computers within an organisational LAN/DMZ like many other trojans, but also vertically out to the Internet as a traditional network worm).



The Trojaned Computer

Once it has successfully infected a computer, the trojan will typically 'phone home' to a command and control (C&C) centre. There are many ways it can do this. Historically, the ICQ protocol was popular amongst trojan writers, but we've also seen trojans use DNS and other messaging protocols. Some even use the TOR network to disguise their activity. Nowadays, the majority of trojans communicate with their C&C over the HTTP or HTTPS protocols.

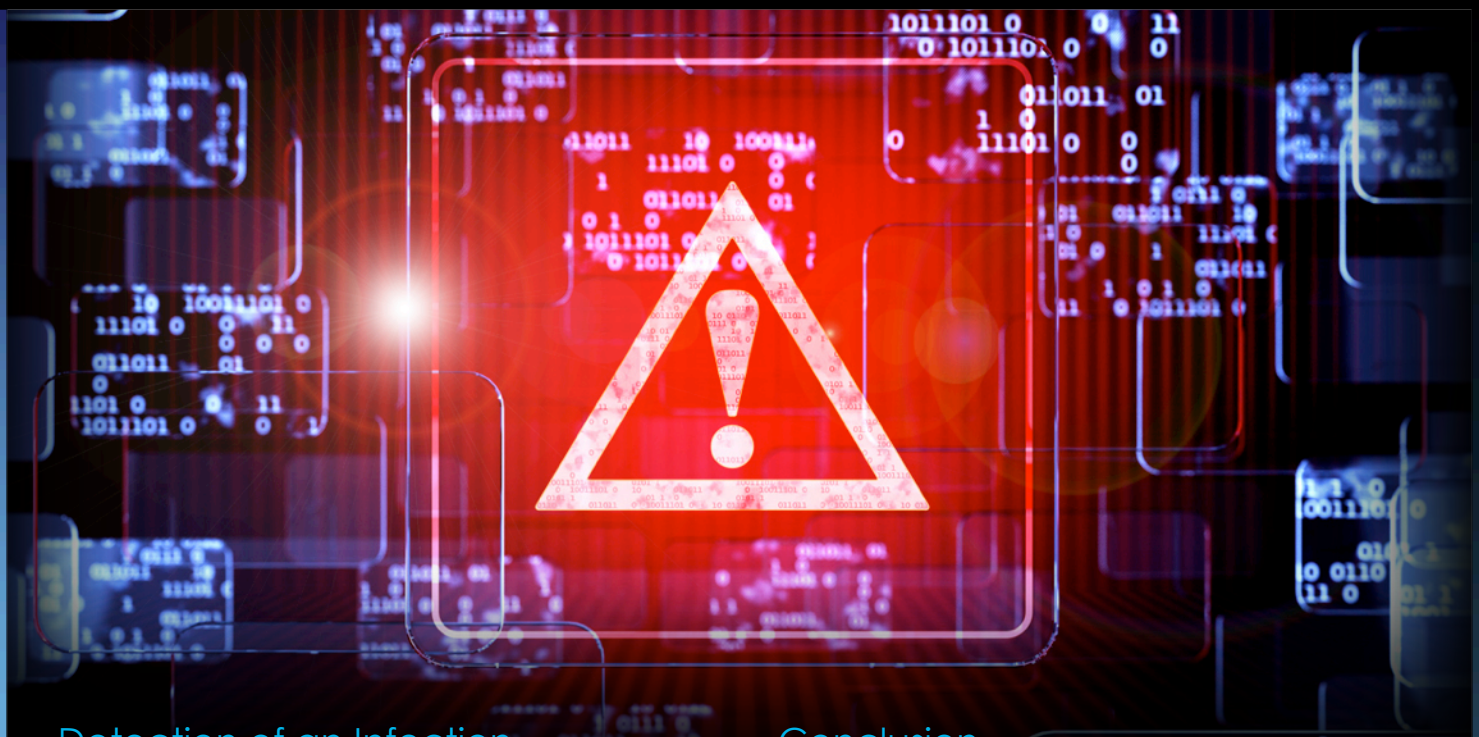
The behaviour of the 12,000+ different types of trojans can be vastly varied, but in general the trojan either uses the infected computer as part of a large botnet (for spamming, malware distribution, DDoS, or other such behaviour), or attacks the infected computer itself to ransom the data for financial gain.

Protection against Initial Infection

So, how can we protect against trojan infection? This is best done by effective scanning and policy control at the gateway:

1. Employ anti-malware protection to scan eMail (SMTP, POP3, IMAP4) and web (HTTP, HTTPS) protocols that the trojan downloaders use to get in.
2. Employ anti-spam protection to scan eMail (SMTP, POP3, IMAP4) protocols.
3. Design your inbound firewall rules to block-off incoming ports from the Internet - only allow what is specifically required, and never open 'dangerous' ports such as ssh, telnet, smb.
4. Use IPS systems to scan inbound traffic and block known exploits.
5. Use effective policy control - block emails containing executable attachments such as Microsoft Office documents with macros.
6. Patch. Patch. Patch. Often and Early. Keep your systems up-to-date with the latest manufacturer-supplied patches.
7. Obsolete and unmaintained systems should not be allowed on the network.
8. Disable all unnecessary services.
9. Deploy multi-level defense both at the gateway and at the end-point devices.

NETWORK BOX



Detection of an Infection

Should a trojan downloader get into your network, there are various technologies that can be used to detect the issue and stop it's spread:

1. Use IDS/IPS systems to scan outbound traffic and alert on known command-and-control traffic.
2. Use InfectedLAN systems to detect and alert on communications with known command-and-control centres.
3. Design your outbound firewall rules to restrict outbound access and deny potentially dangerous protocols such as TOR.
4. Use effective policy control on your internal network - such as segmenting your network using VLANs to isolate high-value from high-risk systems.

Preparation for an Infection

It is not just about the box. While Network Box 5 offers both signature and heuristics based anti-malware scanning, firewall policy enforcement, IPS, IDS, and Infected LAN systems, there is still the chance that somebody will plug an infected laptop into your network, bring in a USB key, or download a trojan via something such as encrypted Skype communications. The single most important thing you can do to prepare for an Infection, is exactly what you should be doing anyway - implement an effective and secure file backup policy.

You should be keeping at least three copies of all important files on your network:

1. The file itself
2. An on-site backup copy
3. An off-site, off-line, backup copy

Conclusion

Follow industry standard practices for this to ensure that (a) all important files are part of the backup policy, (b) the backups are rotated to maintain a history, (c) the off-site backups are transported appropriately, (d) the backups are periodically tested, and (e) the entire backup system is documented and logs maintained. You should be doing this anyway. After all, the chances of a hard disk failure are probably higher than those of ransomware infection (so long as you are following the above protection and detection steps).

Planning for a Trojan / Ransomware attack is not just about the protection and detection systems you deploy at the gateway. The military has an adage called the 7 Ps - Proper Planning and Preparation Prevents Piss Poor Performance – adhering to such advise may just save you one day. Once you have your plan in place, communicate it to your partners (security and other service providers) as well as internally. Then, file it away in a place you can get to should the unthinkable happen.

NETWORK BOX

TA17-156A: Reducing the Risk of SNMP Abuse

References
The Interfaces Group MIB using SMIv2:
https://www.ietf.org/rfc/rfc2233.txt

Revision History
June 5, 2017: Initial Release

The US-CERT and Department of Homeland Security has released a National Cyber Awareness System alert TA17-156A regarding SNMP Abuse. We recommend that all Network Box users heed this advise. Network Box 3 and 5 do not use or enable SNMP by default, but it is available to customers that require it. If you enable it, please make sure it is configured in a secure manner.

Systems Affected

SNMP enabled devices.

Overview

The Simple Network Management Protocol (SNMP) may be abused to gain unauthorized access to network devices. SNMP provides a standardized framework for a common language that is used for monitoring and managing devices in a network.

This Alert provides information on SNMP best practices, along with prevention and mitigation recommendations.

Description

SNMP depends on secure strings (or "community strings") that grant access to portions of devices' management planes. Abuse of SNMP could allow an unauthorized third party to gain access to a network device.

SNMPv3 should be the only version of SNMP employed because SNMPv3 has the ability to authenticate and encrypt payloads. When either SNMPv1 or SNMPv2 are employed, an adversary could sniff network traffic to determine the community string. This compromise could enable a man-in-the-middle or replay attack.

Although SNMPv1 and SNMPv2 have similar characteristics, 64-bit counters were added to SNMPv2 so it could support faster interfaces. SNMPv3 replaces the simple/clear text password sharing used in SNMPv2 with more securely encoded parameters. All versions run over the User Datagram Protocol (UDP).

Simply using SNMPv3 is not enough to prevent abuse of the protocol. A safer approach is to combine SNMPv3 with management information base (MIB) whitelisting using SNMP views. This technique ensures that even with exposed credentials, information cannot be read from or written to the device unless the information is needed for monitoring or normal device re-configuration. The majority of devices that support SNMP contain a generic set of MIBs that are vendor agnostic. This approach allows the object identifier (OID) to be applied to devices regardless of manufacturer.

Impact

A remote attacker may abuse SNMP-enabled network devices to access an organization's network infrastructure.

Solution

A fundamental way to enhance network infrastructure security is to safeguard networking devices with secure configurations. US-CERT recommends that administrators:

- Configure SNMPv3 to use the highest level of security available on the device; this would be *authPriv* on most devices. *authPriv* includes authentication and encryption features, and employing both features enhances overall network security. Some older images may not contain the cryptographic feature set, in which case *authNoPriv* needs to be used. However, if the device does not support Version 3 *authPriv*, it should be upgraded.
- Ensure administrative credentials are properly configured with different passwords for authentication and encryption. In configuring accounts, follow the principle of least privilege. Role separation between polling/receiving traps (reading) and configuring users or groups (writing) is imperative because many SNMP managers require login credentials to be stored on disk in order to receive traps.
- Refer to your vendor's guidance for implementing SNMP views. SNMP view is a command that can be used to limit the available OIDs. When OIDs are included in the view, all other MIB trees are inherently denied. The SNMP *view* command must be used in conjunction with a predefined list of MIB objects.
- Apply extended access control lists (ACLs) to block unauthorized computers from accessing the device. Access to devices with read and/or write SNMP permission should be strictly controlled. If monitoring and change management are done through separate software, then they should be on separate devices.
- Segregate SNMP traffic onto a separate management network. Management network traffic should be out-of-band; however, if device management must coincide with standard network activity, all communication occurring over that network should use some encryption capability. If the network device has a dedicated management port, it should be the sole link for services like SNMP, Secure Shell (SSH), etc.
- Keep system images and software up-to-date.

Network Box 5

NEXT GENERATION MANAGED SECURITY

On Tuesday, 6th June 2017, Network Box will release our patch Tuesday set of enhancements and fixes. The regional SOCs will be conducting the rollouts of the new functionality in a phased manner over the next 14 days.

Network Box 5 Features
June 2017

This month, for Network Box 5, these include:

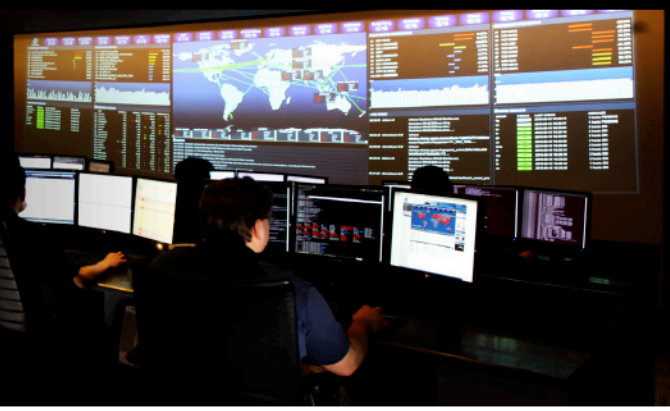
- Improvements to reliability of rebooting/ shutdown device under high memory utilization conditions
- Enhancements to disk utilization summary report for high workload deployments
- Introduction of averaging for per-minute statistics with less than 60 seconds of data available
- Support for the new UTM-5Q and VPN-5Q box models
- Performance improvements to URL categorization
- Introduce support for direct searching by holistic record ID in admin web portal
- Switch of signature downloads to use new global CDN for improved download speed
- Improvements to GMS sensor for system logging
- General layout improvements in Admin and User web portals
- Improvements to saving of modified widget filters in Admin and User web portals
- Performance improvements in User web portal
- Support for sender-dependant routing maps for mail server security module
- Enhanced support for SMTP third party relay protection of forward-path addresses
- General improvements to NOC secure maintenance connections and remote device control
- A large batch of core system updates

In most cases, the above changes should not impact running services or require a device restart. However, in some cases (depending on configuration), a device restart may be required. Your local SOC will contact you to arrange this if necessary.

Should you need any further information on any of the above, please contact your local SOC. They will be arranging deployment and liaison.

NETWORK BOX

Network Box ISO 9001 / ISO 20000 / ISO 27001 certified Security Operations Centre, ensures that customers' networks are protected against cyber threats, 24x7x365.



Network Box Hong Kong
Redefining Hong Kong Debate Series

Network Box Managing Director, Michael Gazeley, was a guest panelist at the 5th SCMP Redefining Hong Kong Debate Series, featuring constructive dialogue and analysis on issues that are affecting the city. The event, which was organized and moderated by the South China Morning Post, took place at the JW Marriott Hong Kong.

Network Box Australasia
CERT NZ Launch Event

Network Box Australasia was at the launch of the New Zealand government's Computer Emergency Response Team (CERT NZ). Over 200 people attended the event which took place at the Ministry of Business, Innovation and Employment, in Wellington, New Zealand.

Network Box Media Coverage:
WannaCry Ransomware

In light of the recent WannaCry Ransomware, where over 300,000 systems in over 150 countries were affected, Michael Gazeley, Network Box Managing Director, was interviewed by various media outlets, to share his thoughts and views on the outbreak.

What is ransomware?
http://money.cnn.com/2017/05/15/technology/ransomware-wannacry-explainer/

Global ransomware attack: 5 things to know
http://edition.cnn.com/2017/05/13/world/ransomware-attack-things-to-know/index.html

Some businesses in Asia disrupted by cyber attack, authorities brace for more
http://www.reuters.com/article/cyber-attack-idUSL4N1IH12R

WannaCry ransomware cyber-attacks slow but fears remain
http://www.bbc.com/news/technology-39920141

Impact of global cyberattack could strike Hong Kong on Monday morning
http://www.scmp.com/news/hong-kong/law-crime/article/2094222/impact-global-cyberattack-could-strike-hong-kong-monday

Tens of thousands of Chinese firms, institutes affected in WannaCry global cyberattack
http://www.scmp.com/news/china/policies-politics/article/2094377/tens-thousands-chinese-firms-institutes-affected

HK officials in the dark about ransomware: expert
http://news.rthk.hk/rthk/en/component/k2/1331051-20170518.htm?spTabChangeable=0

Newsletter Staff	Subscription
Mark Webb-Johnson Editor **Michael Gazeley** **Nick Jones** **Kevin Hla** Production Support **Network Box HQ** **Network Box USA** Contributors	Network Box Corporation nbhq@network-box.com or via mail at: **Network Box Corporation** 16th Floor, Metro Loft, 38 Kwai Hei Street, Kwai Chung, Hong Kong Tel: +852 2736-2083 Fax: +852 2736-2778 www.network-box.com