Advanced Malware Risk Report

Prepared for Cisco Customer Forum

Friday 07 March 2014

Prepared by Leon Ward, Cisco Channel Partner

Contact: leonward@cisco.com

I. EXECUTIVE SUMMARY

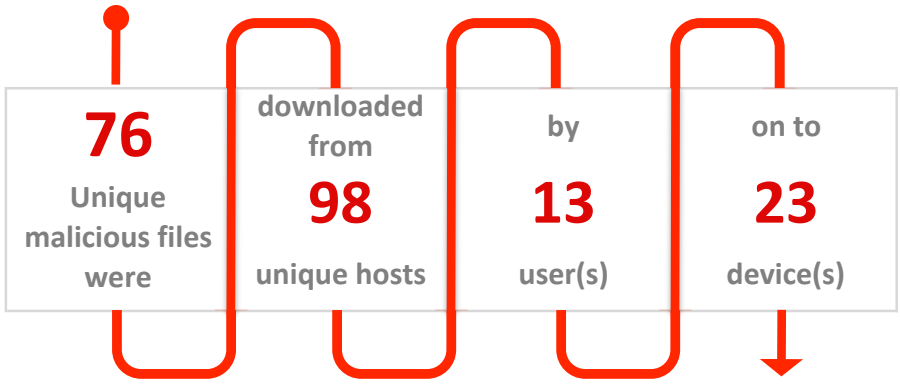
Sourcefire has determined that Cisco Customer Forum is at a High risk due to the observation of attack by 22 different families of malware. Sourcefire Advanced Malware Protection for FirePOWER was deployed for an assessment period of 100 days. This report is a record of what was found on the network during this time

Assessment Period: Wed Nov 27 15:31:14 2013 to Fri Mar 7 15:31:14 2014

Malware Families	**Hosts displaying IoCs**	**Infection Protocols**
29	**98**	**6**
Hosts Connected to CnC Servers	**Malware Comms**	**Malware URLs**
12	**6,556**	**14**

(A summary of the assessment results starts on page 3)

MALWARE PROFILE: OVER THE LAST 100 DAYS



Sourcefire recommends that Advanced Malware Protection for FirePOWER is deployed to:

1. Establish continuous visibility into advanced malware
2. Augment existing controls in order to mitigate this risk

SOURCEfire

II. ASSESSMENT RESULTS

HOSTS DISPLAYING INDICATIONS OF COMPROMISE

Special attention should be paid to computers showing indications of compromise as they are likely to be exfiltrating information from your private systems. Systems that fall into this category likely have had malware residing on them for some time already and the initial infection has been missed by existing security protections, or are under current attack.

HOST ADDRESS	IOC COUNT
10.0.108.18	4
10.0.108.11	4
10.0.108.24	4
10.0.108.16	4
10.131.15.45	3

TOTAL HOSTS CONNCTED TO BOTNET C&C SERVERS (details on next page)
12

COMMON INDICATIONS OF COMPROMISE FOUND

Indications of compromise take many forms, perhaps a host has been seen to execute malware, be connected to a Command & Control server, be targeted with a high impact attack, or actively leaking data. Across the monitored network, these are a sample of different IoCs detected against live systems.

MOST COMMON IOC TYPES DISCOVERED

IOC CATEGORY	IOC DESCRIPTION	COUNT
Malware Detected	The host has encountered malware	2839
Impact 2 Attack	The host was attacked and is potentially vulnerable	322
Impact 1 Attack	The host was attacked and is likely vulnerable	12
Malware Executed	The host has executed malware	7
Dropper Infection	The host may be infected with Dropper	7

HOSTS CONNECTED TO COMMAND AND CONTROL SERVERS

The following devices have been identified as being connected to command and control (CNC) servers. Sourcefire detects CNC detections through a mix of deep packet (content) inspection, network communications to hosts identified by the VRT as hosting CNC infrastructure and connections outbound from processes on an endpoint that are known to be malicious.

SAMPLE OF HOSTS CONNECTED TO CNC SERVERS

IP ADDRESS	IP ADDRESS
192.168.42.1	192.168.33.1
192.168.44.15	121.42.14.5
10.34.52.1	33.43.1.4
193.13.44.4	192.168.33.11
23.41.55.1	192.33.5.1

MALWARE FOUND ON THE NETWORK

Top threats seen in your environment should be researched because they may affect your security exposure. You should take action to remove and prevent reintroduction by these specific threat types:

FILE BASED MALWARE DETECTIONS

MALWARE NAME	NUMBER OF DETECTIONS	NUMBER OF HOSTS
Suspicious_F:Downloader-tpd	11,919	235
Troj_Generic:Small-tpd	10,782	234
W32.Trojan.c8a2	6,096	1,970
Suspicious_Gen3:EraseHDD-tpd	5,249	229
Downloader:Trojano-tpd	4,211	51

SOURCEfire®

III. FILE DETAILS

FILES SEEN MOVING AROUND THE NETWORK

The following files types have been seen moving around the network. To limit your exposure to malware risk it is wise to control data movement my policy. File movement can be controlled by user, group, network zone, app, protocol, file type, and disposition.

FILE CATEGORY	COUNT	CATEGORY	APP
Executables	216,262	MSEXE	HTTP
Office Documents	180,451	MSOLE2	HTTP
PDF files	88,840	PDF	HTTP
Archive	52,383	ZIP	HTTP
Office Documents	44,772	RTF	HTTP

DYNAMIC ANALYSIS & THREAT SCORE

Sourcefire Advanced Malware Protection (AMP) solutions provide detailed analysis of file behavior after execution takes place. A Threat Score is associated with files, this is calculated based on the behavior observed in the dynamic analysis environment.

FILENAME	SHA256 (Unique identifier for file)	THREAT SCORE (/100)
adverts-printout.msexe	590796a0f7fbb2b537119336efea7ad8e54b70bfa6d866060110cc272bb871b7	100
Hiloti.exe	590796a0f7fbb2b537119336efea7ad8e54b70bfa6d866060110cc272bb871b7	100
tangerine-	590796a0f7fbb2b537119336efea7ad8e54b70bfa6d866060110cc272bb871b7	100
Renos.exe	590796a0f7fbb2b537119336efea7ad8e54b70bfa6d866060110cc272bb871b7	100
Lovgate.exe	590796a0f7fbb2b537119336efea7ad8e54b70bfa6d866060110cc272bb871b7	100
Gael.exe	590796a0f7fbb2b537119336efea7ad8e54b70bfa6d866060110cc272bb871b7	100
Nuqel.exe	590796a0f7fbb2b537119336efea7ad8e54b70bfa6d866060110cc272bb871b7	100
FakeScanti.exe	590796a0f7fbb2b537119336efea7ad8e54b70bfa6d866060110cc272bb871b7	100
Bagz.exe	590796a0f7fbb2b537119336efea7ad8e54b70bfa6d866060110cc272bb871b7	100
Bubnix.exe	590796a0f7fbb2b537119336efea7ad8e54b70bfa6d866060110cc272bb871b7	100

DYNAMIC ANALYSIS EXAMPLE OUTPUT

Below is an example of dynamic analysis output taken from one file found on your network. This file had a threat score of 100 out of 100. A more detailed analysis of this file is available in the Defense Center along with screenshots, network traffic it generated, and files it may have also dropped.

EXAMPLE SHA256 590796a0f7fbb2b537119336efea7ad8e54b70bfa6d866060110cc272bb871b7

OBSERVATION	SCORE
* AV Detection	1
- VirusTotal Search Results	1
* Persistence and Installation Behavior	100
- Drops PE files	100
* System Summary	39
- Creates temporary files	10
- Executable uses VB runtime library 6.0 (Probably coded in Visual Basic)	5
- Creates files inside the system directory	100
* Anti Debugging	100
- Found dropped PE file which has not been started or loaded	100
* E-Banking Fraud	100
- Found strings which match to known bank urls	30
* Networking	20
- Urls found in memory or binary data	10
- Found strings which match to known social media urls	40

III. MALWARE RISK TO THE BUSINESS

IMPACT OF MALWARE TYPES

Malware exposes different types of risk to the organisation that encounters it. Malware is commonly categorized into different types that enable the security team to deal with the Immediate threat. Below are different types of malware commonly discovered by Sourcefire solutions.

MALWARE TYPE	RISK TO BUSINESS
Botnet client	Denial of Service, Information Theft. A botnet is a collection of computers controlled by a third party. Hosts controlled by a botnet may steal information from your organization or be used to launch denial-of-service attacks, send spam, or conduct other undesirable activity.
Trojan / Backdoor	System Degradation, Information Theft: A trojan horse is a program that appears to be benign to an end user but is in fact malicious. It can be used to steal information or introduce control
Spyware	Information Theft: Spyware is software installed on machines that collects information without users' knowledge and forwards it to other organizations.

IV. RECOMMENDATIONS

Despite your existing network and endpoint protections, advanced malware is getting through and placing your organization at risk. Additional countermeasures and security controls are required to mitigate the risk.

Sourcefire recommends that Cisco Customer Forum deploy FirePOWER Appliances with Advanced Malware

1. Establish continuous network visibility into its advanced malware risk
2. Augment its existing controls in order to mitigate this risk
3. Add host protection and enhanced remediation via FireAMP connectors

1. ESTABLISH CONTINUOUS MALWARE VISIBILITY

Existing protections are neither dynamic enough nor capable of fully protecting from new or unknown threats that emerge daily. Sourcefire recommends deployment of network-based protections via FirePOWER Appliances with Advanced Malware Protection. Advanced Malware Protection is a license that you can add to any NGFW or NGIPS appliance from Sourcefire. This will provide the following new capabilities and benefits:

NEW CAPABILITY	BENEFIT
Network Based Detection	Detect and block advanced malware from existing network IDS/IPS infrastructure
Trend Analysis	Measure and see how effective your protections are over time
Cloud-Based Analytics	Powerful cloud analytics leverages Sourcefire's vast security intelligence and expertise without complex or costly deployment
Full-stack Visibility	Understand, at all architecture layers, which hosts, applications and users are involved in risky or malicious activity - use this knowledge to easily develop effective controls and inspection policies.
File Identification	Identify and understand the file types traversing your networks and employ intelligent decisions based on Sourcefire reputational data
Virtual Protection	Monitor VM-to-VM communications the same as physical networks

2. AUGMENT CONTROLS TO MITIGATE RISK

Deploying additional countermeasures can help mitigate the risk advanced malware poses. These measures may entail control of threat surface, blocking entry and propagation of malware or suspect file types, and rapid notification upon new malware discovery.

Sourcefire recommends deployment of network-based protections via FirePOWER Appliances with Advanced Malware Protection. These provide the following new capabilities and benefits:

NEW CAPABILITY	BENEFIT
24/7 Real-Time Protection	Deploy in-line for continuous network protection and minimize propagation of advanced malware
IP Blacklisting	Block Bot C&C, open proxy, and custom IP lists from your IPS
Retrospective Alerting	Alert on files deemed malicious by the Sourcefire Security Intelligence cloud even after infection - leverage community awareness to know when you may be at risk of infection

SOURCEfire®

3. ADD HOST PROTECTION & ENHANCED REMEDIATION VIA FIREAMP

Typically advanced malware enters the network via hosts (compromised end devices such as PCs, smartphones, etc.). Having a presence at the host/client-side OS enables easier determination of root cause, malware trajectory, and more control over the spread of malware (even after a compromise!). It also helps to speed post-infection clean-up efforts.

Sourcefire recommends considering FireAMP Advanced Malware Protection Connectors for additional visibility and control. These provide the following new capabilities and benefits:

NEW CAPABILITY	BENEFIT
Host Protection	Deploy Sourcefire FireAMP Connectors to gain additional protection and more capability to take action against malware at the host.
Mobile Protection	Protect mobile workers and Android-based devices from advanced malware attacks
Virtual Protection	Protect Virtual Desktop communications the same as physical networks
Malware Trajectory	Understand how malware enters and trace the path of infection to identify 'patient zero'
File Analysis	Get more information on how malware behaves, the original file name, screen shots of the malware executing, and sample packet captures
Retrospective Detection	Recall files deemed malicious by the Sourcefire Security Intelligence cloud even after infection - automate and speed malware cleanup

In addition, Sourcefire offers NGIPS capabilities and optional Application Control and URL Filtering, to help better protect against the latest threats. Please contact your Sourcefire representative or reseller for more information.

SOURCEfire®

ABOUT SOURCEFIRE

Sourcefire Inc. (Nasdaq: FIRE), a world leader in intelligent cybersecurity solutions, is transforming the way global large- to mid-size organizations and government agencies manage and minimize network security risks. With solutions from a next-generation network security platform to advanced malware protection, Sourcefire provides customers with Agile Security TM that is as dynamic as the real world it protects and the attackers against which it defends.

Trusted for more than 10 years, Sourcefire has been consistently recognized for its innovation and industry leadership with numerous patents, world- class research, and award winning technology. Today the name Sourcefire has grown synonymous with innovation, security intelligence and agile end-toned security protection.

CONTACT US

Want to learn more about getting this information on your network? Go to http://info.sourcefire.com and request a live demo.