Cisco Solution Protects Before, During, and After Attack

Cisco Cloud Web Security Premium helps global oil and gas company discover and resolve persistent ransomware infection.

Challenges

Content security has never been more challenging in an era where the theft or compromise of corporate data is often the primary incentive for an attack. According to the Cisco 2014 Annual Security Report, Cisco researchers found that 100 percent of business networks they analyzed had traffic going to websites that host malware.[1] They also determined through their observation of this activity that when these networks had been penetrated, it was likely that they had been compromised for some time and that the core infiltration had not been detected.[2]

The following factors are making it especially difficult for security teams to prevent and detect threats:

- **Mobility and cloud**, without proper security measures, are reducing visibility and increasing security complexity. As more organizations embrace cloud computing, virtualization, mobile and remote working, and the bring-your-own-device (BYOD) trend, more and more data is moving outside of enterprise control. The network is becoming more porous, creating more vectors for attack. And as more business-critical services are moved to the cloud and accessed outside of the company's secured perimeter, the attack surface will only continue to expand.
- **Advanced adversaries**, according to the *Cisco 2014 Annual Security Report*, are "proactively working to understand what type of security solutions are being deployed and shifting to less visible, less content-detectable patterns of behavior so their threats are well concealed."[3] This strategy means less "low-hanging fruit" is available for security solutions and professionals to detect, and organizations will face "more cipher traffic, more scrambling, and more randomization by malicious actors to make command-and-control (C&C) behaviors indistinguishable from real traffic."[4]

CUSTOMER PROFILE

Industry: Oil and Gas
Employees: ~15,000
Operations: Global
Security personnel: 12
Other security measures: Antivirus, Firewall, Intrusion Detection System (IDS), Security Information and Event Management (SIEM)

CHALLENGE

- Detect advanced threats delivered through web-based traffic, which can evade legacy security solutions and become embedded in the corporate network
- Develop actionable intelligence to help security team prioritize threats
- Identify single solution that can be deployed across distributed environment, integrate with existing security infrastructure, and provide protection across entire attack continuum

SOLUTION

- Cisco CWS Premium, which includes all features in Cisco CWS Essentials
- Cognitive Threat Analytics (CTA) and Advanced Malware Protection (AMP) to automate search for high-risk threats in web traffic and provide visibility into advanced attacks actively operating in corporate network

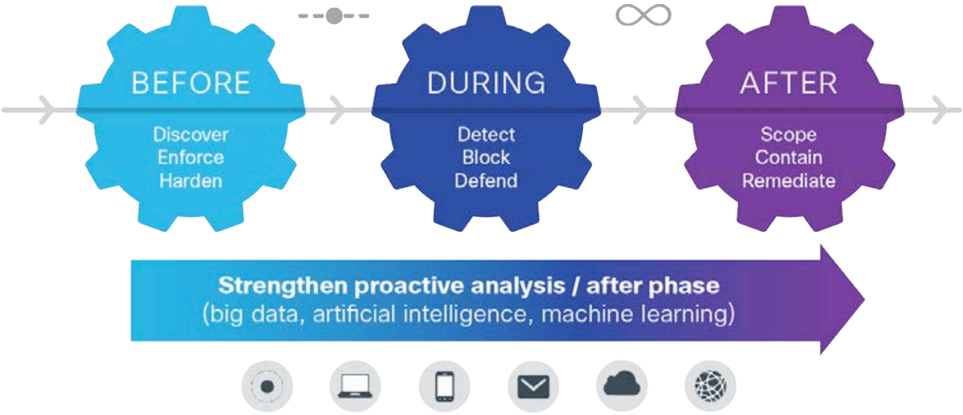
RESULTS

- Persistent and previously undiscovered malware infection identified and resolved
- Threat protection now exists across the entire attack continuum
- Customer's security team can now focus on addressing the most significant threats

[1] *Cisco 2014 Annual Security Report*: http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf.
[2] Ibid.
[3] Ibid.
[4] Ibid.

The complex and continually evolving threat landscape makes discovery more relevant than defense as a modern approach to content security. Today's enterprises must focus on content inspection, behavioral anomaly detection, and advanced forensics to gain visibility into threats that are already present in their networks—the "after" phase of an attack.

Figure 1. New security model: continous security after attack


BEFORE
Discover
Enforce
Harden
DURING
Detect
Block
Defend
AFTER
Scope
Contain
Remediate
Strengthen proactive analysis / after phase
(big data, artificial intelligence, machine learning)

Cisco® Cloud Web Security (CWS) Premium helps organizations meet the challenge of maintaining continuous security across the extended network. A cloud-based version of Cisco Web Security, Cisco CWS is a platform that extends web security to mobile devices and distributed environments. It protects all users through the Cisco worldwide threat intelligence, advanced threat defense capabilities, and roaming-user protection. It includes all of the features in Cisco CWS Essentials, and also combines two innovative malware detection systems to automate the search for high-risk threats in web traffic:

- **Cognitive Threat Analytics (CTA)** is a near-real-time network behavior analysis system that uses machine learning and advanced statistics to spot unusual activity on a network—indicators of compromise (IOCs). CTA spots anomalies and then directs security analysts toward potential problems, helping them to reduce their workload and prioritize threats.
- **Advanced Malware Protection (AMP)** uses a combination of file reputation, file sandboxing, and retrospective file analysis to identify and stop threats across the attack continuum.

The combination of these solutions enables CWS Premium to identify new command-and-control channels not previously detected by the security industry.

This case study examines how CWS Premium helped a global oil and gas company to:

- Gain more visibility into a large and increasing volume of web traffic (more than 35 million HTTP/HTTPs requests per day).
- Generate actionable threat intelligence that is easier for the threat response team to prioritize.
- Deploy a single solution that integrates with existing security infrastructure, and provides protection across the entire attack continuum—before, during, and after an attack.

Solution

Cisco recommended that the customer upgrade to CWS Premium, which includes CTA and AMP, to gain more visibility into its network and help the threat response team prioritize threats.

AMP’s retrospective analysis can reveal that files deemed “clean” when they pass through perimeter defenses are actually well-disguised, advanced malware. AMP immediately alerts the security administrator and provides visibility into which user on the network may have been infected and when.

CTA, meanwhile, detects even stealthier threats that have penetrated defenses and are actively operating in the corporate network. It is an innovative malware detection system that uses behavioral analysis and anomaly detection to pinpoint compromised devices. CTA relies on advanced statistical modeling and machine learning to identify new threats independently, learning from what it sees and adapting over time, without the need for tuning or configuration.

CTA identified evidence of malware activity on the customer’s network and reported it. The malware consisted of a collection of modules controlled by one malware entity. In this case, the payload was Cryptolocker ransomware, a type of malware that encrypts files on victims’ computers and “locks” their device until they pay a ransom.[5]

As illustrated in Figure 2, the adversary operated a command-and-control infrastructure to carry out the attack. Four key steps were involved in this campaign:

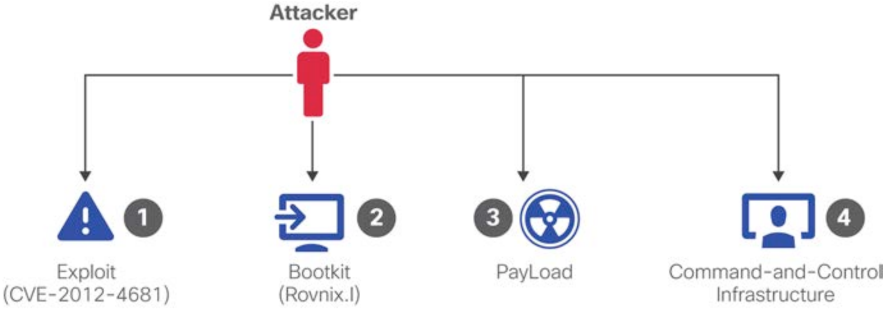
Step 1. The attacker used an exploit (CVE-2012-4681) to take advantage of a vulnerability in the Java Runtime Environment (JRE) component in Oracle Java SE 7 Update 6; this enabled the attacker to execute code remotely, bypassing the security manager.

Step 2. Next, the bootkit (Rovnix.I) was installed to ensure persistence on the machine.

Step 3. The payload was then delivered, making the malware fully operational. (In this case, the payload was Cryptolocker ransomware.)

Step 4. The attack established command-and-control channels to keep the operation active.

Figure 2. Four key steps in the attack

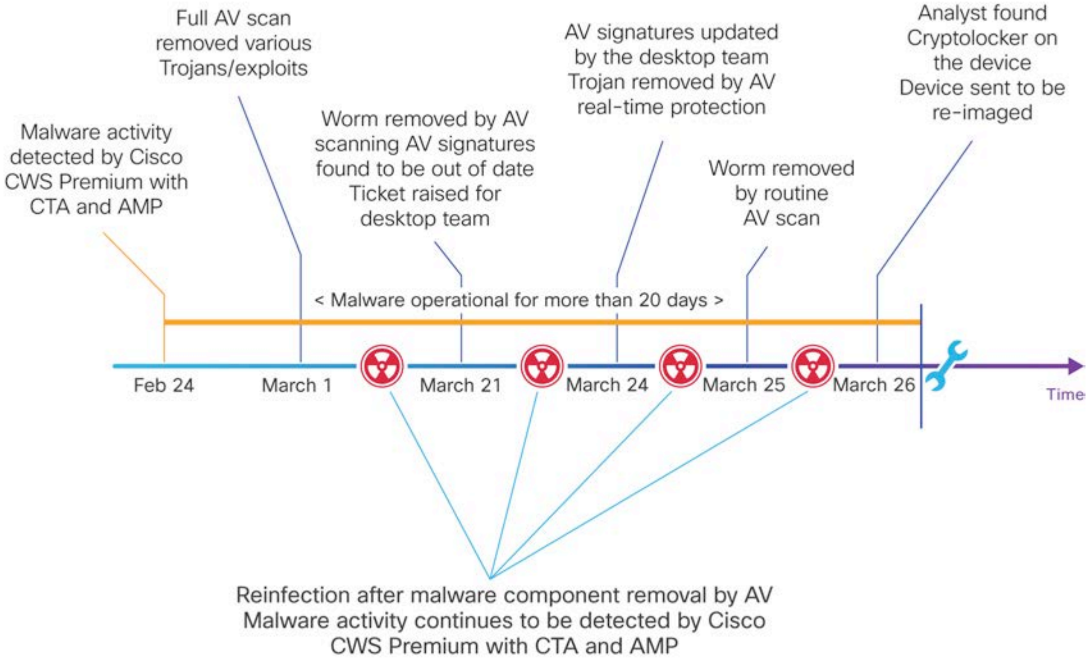


[5] Malvertising, online advertising used to spread malware, played a key role in the distribution of Cryptolocker, which has since been neutralized; malvertising and ransomware are still prevalent threats, however, and are being used by adversaries to launch highly targeted campaigns via the web. For more details, see the Cisco 2014 Midyear Security Report: http://www.cisco.com/web/offer/grs/190720/SecurityReport_Cisco_v4.pdf.

The customer's security team tried to resolve the threat with AV tools. However, because this was a rootkit infection, malware was deeply embedded in the infected system. The AV solution was only able to eliminate some malware components. Until the infection was completely resolved, CTA continued to alert the security team to the presence of persistent malicious activity.

Figure 3 outlines the full timeline from detection of the malware activity to resolution of the threat.

Figure 3. Malware activity timeline: detection to resolution


Full AV scan removed various Trojans/exploits
Malware activity detected by Cisco CWS Premium with CTA and AMP
Worm removed by AV scanning AV signatures found to be out of date Ticket raised for desktop team
AV signatures updated by the desktop team Trojan removed by AV real-time protection
Worm removed by routine AV scan
Analyst found Cryptolocker on the device Device sent to be re-imaged
< Malware operational for more than 20 days >
Feb 24
March 1
March 21
March 24
March 25
March 26
Time
Reinfection after malware component removal by AV Malware activity continues to be detected by Cisco CWS Premium with CTA and AMP

The situation that the customer experienced demonstrates the value of having CWS Premium in operation in the "after" phase of an attack. It also underscores why mitigating advanced attacks using AV products is difficult. The CTA system provided evidence of the ongoing active command-and-control channels. Additionally, it identified several other domains used in the exfiltration of data. Such infections represent long-term breaches buried within the customer infrastructure.

Results

In today's world, where security teams must manage a high volume of incidents daily, no time is available to search for "a needle in a haystack." Security teams need help focusing on the most advanced attacks, and the CTA system is designed to detect and categorize such attacks.

In the case of the customer's Cryptolocker ransomware infection, CWS Premium detected malware activity and applied existing security intelligence to block some of the command-and-control channels attempted by the infected device. However, the attacker then used an additional IP address with unknown reputation; this new channel was operational throughout the infection. This example underscores the strengths (auto-blocking) and weaknesses (new channels are not blocked) of relying on signature-based and web reputation-based detection alone, and why continuous protection after an attack is necessary.

Following is analysis of the command-and-control channels identified by the CTA system in CWS Premium, along with sample web-traffic requests and statistics:

Table 1. Attack infrastructure

Order	Remote server	Destination IP	Destination country	Number of requests	Activity status
1	C&C server #1	109.XXX.XXX.XXX	Netherlands	17 (attempts)	BLOCKED by web reputation
2	**C&C server #2**	**94.XXX.XXX.XXX**	**Luxembourg**	**75**	**ACTIVE CHANNEL**
3	C&C server #3	fistristy.com	Luxembourg	175 (attempts)	BLOCKED by web reputation
4	C&C server #4	ffeed5.com	Russia	7 (attempts)	BLOCKED by web reputation

Table 2. Threats identified by CTA that have subsequently been removed from the device

Threat name	Removed
Cridex Worm	March 19
Cridex.E worm	March 19
Tesch.B trojan	March 19
Java Exploit/CVE-2012-4681	March 19
Trojan downloader Win32/Upatre	March 19
Cridex worm	March 21
Trojan Win32/Viknok.C	March 24
Cridex worm	March 24
Crypto Defense	March 26

Communication to C&C Server # 1 (109.XXX.XXX.XXX)

Communication characteristics:

- Total number of attempted requests to the server was 17; all were C&C communication and blocked by reputation.
- The requests were detected by CTA as attempts to use URL String as Communication Channel (C&C). The URL (shown below in “Example of HTTP request”) represents an encoded message. Similar structure of the URL string (IP address/m/IbQ.*) was shared by multiple URLs used in this attack. The fact that the communication was blocked by the reputation system adds even more contextual evidence.
- The attacker also set up a second C&C channel on a server that was not yet part of the reputation feeds to ensure the malware remained operational. The URL itself is an encoded message.

Example of HTTP request (anonymized and truncated)

```
http://109.XXX.XX.XXX/m/IbQXXXVjjpcE6+54HXXXdmmGcNZxtMZdvqyB5EkJAUmL/1sOXXXvq5zzXtIu9SzgnJhj
WlxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXX.g+fq4XXX
OTYke6uhGHDOEeqje76v7z7i+wgqXXXFBuMz5k08yocxOH63bwQ9JMfwy8uNRM…
```

<u>Communication to C&C Server #2 (94.XXX.XXX.XXX)</u>

Communication characteristics:

- Total number of requests to this server was 75; all were C&C requests.
- Two C&C attempts were detected by CTA as **HTTP Traffic to IP Address (No Domain Specified)**. This behavior category spots anomalous request(s) representing out-of-sequence communication to a pure IP address. Such activity may be performed by malware as a “keep-alive” check to confirm the malware is still active or to simply exfiltrate data and to receive additional instructions from its malicious infrastructure (C&C). This type of traffic is not produced by normal Internet browsing.
- All 75 C&C requests were not detected by signature-based and reputation-based technologies.

Example of HTTP request (anonymized and truncated)

```
http://94.XXX.XXX.XXX/m/IbQXXXVjj7iA+O54XXXodmmGcNZxtMZdvqyB5EkJAUmLb3pvGIRvqizzXtIu9SzgnJhjW
lxdE7FiqDEYFm5A+TPlXXXQpGhxGu0r3WLZoX1KHnCShKJDAufwiISy69wApgn4e79NFw/108XXXog+fq4XXXaE
0qfJf1FwalZJKnDc7U0H30+XkiXXXIApkslTo5yvM0TkHrZncwIvumxLCQ+fq4XXXOT…
```

Communication to C&C Server #3 (fistristy.com)

Communication characteristics:

- Total number of requests to fistristy.com domain was 175; all were C&C communication.
- The web signature-based and reputation-based technologies blocked all the requests.

Example of HTTP request

hXXp://fistristy.com/aa/

Communication to C&C Server #4 (ffeed5.com)

Communication characteristics:

- Total number of requests to ffeed5.com was seven; all were C&C communication blocked by CWS Premium.
- CTA has detected six requests as **Anomalous HTTP Traffic** category. This behavior category includes malware behavior generally not fitting with the behavioral baseline established by the continuous CTA analysis. The term “baseline” denotes the state of the statistical models built by the CTA system, which “learns” the trends and characteristics of analyzed web traffic. CTA automatically adjusts the baseline as the network is changing (for example, night and day) to provide the best detection results.
- CTA uses long-term modeling of network behavior to correlate seemingly disparate activities together. It then compares that data to individual user behaviors across the customer’s network to enhance discovery capabilities for stealthy and persistent threats.

Example of HTTP request

hXXp://ffeed5.com/cmd?version=1.5&aid=555&id=24c6b407-5010-4d8d-a266-ffdac7d6f901&os=6.1.7601_1.0_64

Conclusion

The customer's security team needed an easier way to monitor activity and prioritize security events on a network with more than 15,000 users and generating over 35 million web transactions per day, on average. The customer also needed a solution that not only can block threats, but also quickly identify those that inevitably slip past other defenses. The customer required technology designed to alert security personnel of the presence of persistent suspicious activity until the threat is fully resolved.

By deploying CTA as part of Cisco CWS Premium, the customer now has a near-real-time network behavior analysis system that uses machine learning and advanced statistics to spot IOCs in the network. In the example of the Cryptolocker ransomware infection, CTA continued alerting on malicious activity until the security team fully addressed the infection. Additionally, the insight that CTA provides into malware behavior enables the customer's security team to focus their attention on addressing only the most significant threats before, during, and after an attack.

Learn more

Cisco CWS Premium, which includes CTA and AMP, aligns with the Cisco strategy to help organizations address known and emerging security challenges by helping them to detect, understand, and stop threats through continuous analysis and real-time security intelligence delivered from the cloud and shared across all security solutions to improve efficacy. The combination of these three solutions enables CWS Premium to identify new command-and-control channels not previously detected by the security industry, and to help organizations address security challenges across the entire attack continuum.

To find out more about CWS Premium, go to http://www.cisco.com/go/cws.

For more information on CTA, see http://www.cisco.com/go/cognitive.

For more on AMP, visit http://www.cisco.com/go/amp.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C36-733153-00 10/14