VOLUME 2017, NUMBER 4

SECUREWORKS® THREAT INTELLIGENCE EXECUTIVE REPORT

PRESENTED BY THE COUNTER THREAT UNIT™ (CTU) RESEARCH TEAM

SecureWorks®

Executive summary

The SecureWorks® Counter Threat Unit™ (CTU) research team analyzes security threats and helps organizations protect their systems. During May and June 2017, CTU™ researchers identified lessons learned and observed notable developments in threat behaviors, the global threat landscape, and security trends:

- The global WCry and NotPetya campaigns reinforced the need for a layered approach to security.
- Attacks used obfuscated malicious files and scripts to bypass filtering and deliver malware.
- A Chinese threat group has had repeated success using compromised websites to attack targeted organizations.
- Threat actors have been stealing intellectual property from Japanese enterprises.

WCry and NotPetya: Global impact, different objectives

In May 2017, organizations around the world were significantly hampered by the WCry (also known as WanaCry, WanaCrypt, and Wana Decrypt0r) ransomware. The CTU research team and other security groups linked the rapid spread of the ransomware payload to exploitation of Windows Server Message Block (SMB) v1 protocol vulnerabilities that Microsoft addressed in its March 2017 security update. CTU researchers believe the campaign was financially motivated and likely perpetrated by a threat group associated with North Korean government cyber operations.

In June 2017, CTU researchers investigated the global NotPetya malware outbreak and independently confirmed that the initial infection vector was a compromised update of the MeDoc financial accounting software. The malware then leveraged a combination of SMB v1 vulnerabilities and stolen network credentials to propagate within networks. NotPetya rendered the data on infected systems inaccessible.

MeDoc is one of two software products approved by the Ukrainian government for tax records, and NotPetya clearly targeted organizations based or operating in Ukraine. CTU analysis suggests that the attack was conducted by a threat group linked to Russian intelligence services, and that it was part of ongoing disruptive activity against Ukraine rather than a financially motivated ransomware attack.

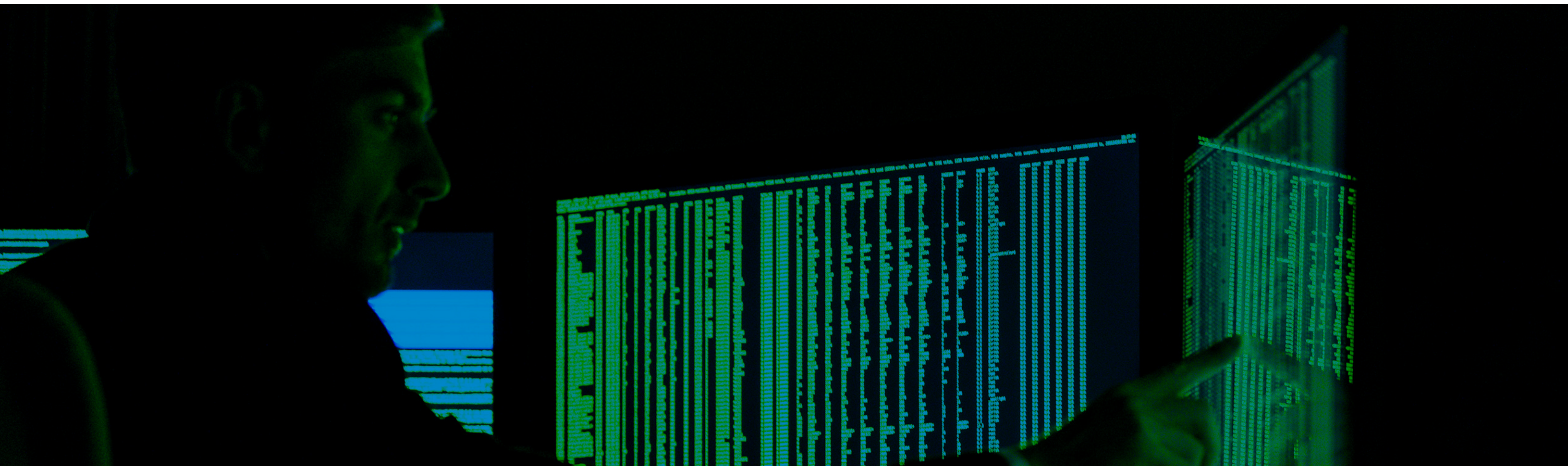
The similarities and differences between these two campaigns highlight the need to adopt a mixture of security controls. For example, patching was necessary but insufficient protection against the spread of the NotPetya malware.

- Apply security updates to operating systems in a timely manner. Both WCry and NotPetya leveraged a vulnerability addressed by Microsoft in March.
- Verify and test third-party patches in isolation where possible. Consider potential risks before implicitly trusting software updates downloaded from the Internet.
- Disable unnecessary protocols. When legacy systems require protocols such as SMBv1, or when hosts cannot be updated, restrict legacy protocols to networks that require the service and isolate them from other hosts on the network.
- Apply the principle of least privilege. Malware often requires enhanced privileges for operations such as credential theft, and the potential for damage is minimized if it cannot run with required permissions.
- Ensure that security policies incorporate best practices for elements such as in-memory credential storage and securing Active Directory.
- Develop and regularly test robust backup and incident response strategies.

Innocuous filenames and extensions used to evade detection

CTU researchers observed three different intrusions that used obfuscated PowerShell scripts to download and execute a loader script for PupyRAT, a publicly available remote access trojan (RAT). The threat actor disguised the scripts as image files (.jpg and .png) and other benign file types (e.g., .msg), and named the scripts after the target organization or programs specific to the organization's industry. In each case, the threat actor abused prior unauthorized access to a host to execute a Base64-encoded PowerShell script, which downloaded the PupyRAT loader script. This PupyRAT loader was also Base64-encoded and had a seemingly legitimate filename. It loaded the PupyRAT tool directly into memory.

The threat actors may have used innocuous filenames and file extensions to bypass web-filtering rules that block downloads of PowerShell or other executable scripts, or to make downloads less conspicuous in network logs. The use of good endpoint security controls, including the deployment of advanced endpoint threat detection (AETD) services, could detect or prevent this activity.



China-based threat group targeted high-profile Turkish organizations

CTU researchers analyzed the activities of the BRONZE UNION threat group (formerly labelled TG-3390), which is likely located in the People's Republic of China. In a mid-2015 campaign, the group used a compromised website to deliver malware to aerospace, academic, healthcare, government, technology, and media network organizations around the world. In November 2016, the group appeared to use the compromised website in a concerted effort to compromise strategically significant networks in Turkey, including networks for government and financial organizations. The range of targeted verticals illustrates the breadth and scale of BRONZE UNION's intent and objectives.

The group has historically made extensive use of strategic web compromise (SWC) attacks to access targeted networks, but it has also used scan-and-exploit techniques as an access vector. After accessing a network, the threat group uses a range of proprietary, publicly available, and native tools to search for and acquire desirable data. CTU researchers recommend that organizations conduct regular internal vulnerability scanning, patching, and upgrading of priority systems to mitigate these threats.

Japanese enterprises targeted in long-running campaign

In a long-running threat campaign targeting enterprises in Japan, the BRONZE BUTLER (also known as Tick) threat group focuses on exfiltrating intellectual property and other confidential data. SecureWorks analysts observed the threat actors operating in Japanese networks involved in critical infrastructure, heavy industry, manufacturing, and international relations.

BRONZE BUTLER leverages spearphishing, SWCs, and a zero-day vulnerability in a popular Japanese corporate software application to compromise targeted systems. The group has developed proprietary malware tools that use encrypted command and control (C2) protocols, which presents analytical challenges for network defenders. After exfiltrating data from a network, BRONZE BUTLER typically deletes evidence of its activities. However, it maintains access to compromised environments, periodically revisiting them to identify new opportunities for data exfiltration.

Although this activity appears to exclusively target Japanese enterprises, the same mitigation techniques can apply to threats in other regions. All organizations should evaluate and manage the risk from threats, implement an AETD solution, and develop incident response plans.

Conclusion

As threat actors increase their level of sophistication, traditional monitoring and detection mechanisms become less effective. Relying on known-bad IP addresses and domain names in web proxy and firewall logs is insufficient because threat groups regularly move infrastructure to evade detection. Intrusion detection system (IDS) and intrusion prevention system (IPS) devices can only detect malicious activity involving known malware. New malware and attacks that abuse stolen credentials are much more difficult to identify.

Using endpoint activity monitoring to identify suspicious behaviors on network endpoints reduces the fallible dependence on specific malware families or reused infrastructure. Endpoint monitoring is often the only way to detect activities such as credential harvesting, edits to registry data, data exfiltration, ransomware installation, and disk wiper attacks. When responding to network intrusions, one of the first actions SecureWorks incident responders often take is deploying AETD - Red Cloak™ to gain insight into activity in the environment and ensure a successful eviction of the threat actor. Organizations without visibility into endpoint activity have limited capability to detect network intrusions, particularly when threat actors use stolen credentials.

A Glance at the **CTU RESEARCH TEAM**

SecureWorks CTU Threat Intelligence

CTU researchers frequently serve as expert resources for the media, publish technical analyses for the security community and speak about emerging threats at security conferences. Our IT security experts also provide Information Security Awareness Training solutions specific to your organizational needs. Leveraging our advanced security technologies and a network of industry contacts, the CTU research team tracks leading hackers and analyzes anomalous activity, uncovering new attack techniques and threats. This process enables CTU researchers to identify threats as they emerge and develop countermeasures that protect our customers before damage can occur.

RESEARCH

Understanding the nature of threats clients face, and creating countermeasures to address and protect.

INTELLIGENCE

Providing information that extends the visibility of threats beyond the edges of a network.

INTEGRATION

Infusing CTU research and intelligence into SecureWorks managed security services and security consulting practices.

SecureWorks®

SecureWorks is a global provider of intelligence-driven information security solutions exclusively focused on protecting its clients from cyberattacks. SecureWorks' solutions enable organizations to fortify their cyber defenses to prevent security breaches, detect malicious activity in real time, prioritize and respond rapidly to security breaches and predict emerging threats.

Corporate Headquarters

1 Concourse Pkwy NE #500
Atlanta, GA 30328
1.877.838.7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France
93218 Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center, Unterschweinstiege 10
60549 Frankfurt am Main
Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
UK House, 180 Oxford St
London W1D 1NN
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City
Dubai, UAE PO Box 500111
00971 4 420 7000

Asia Pacific

Australia
Building 3, 14 Aquatic Drive
Frenchs Forest, Sydney NSW
Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp