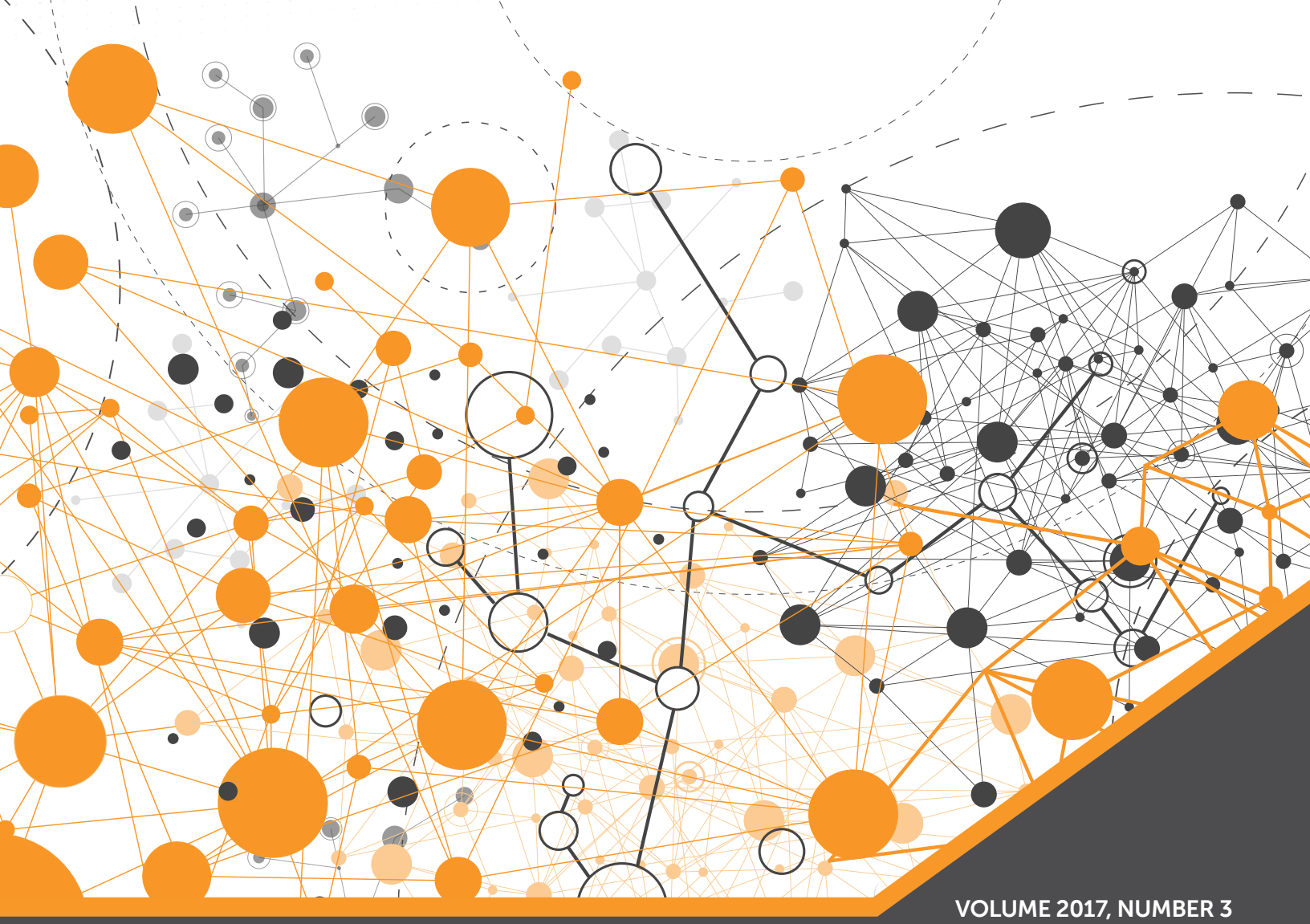
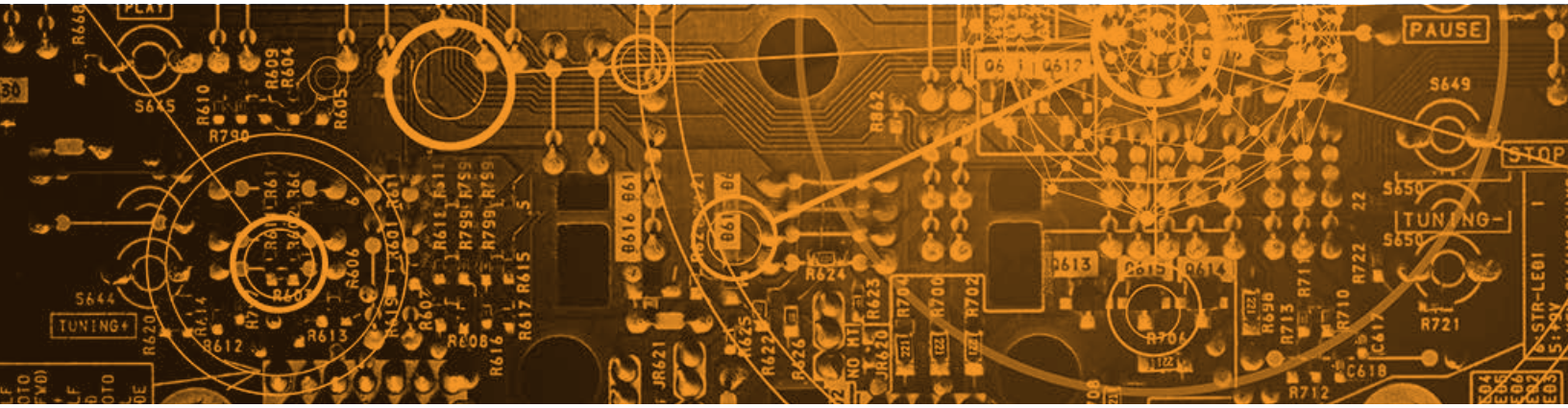


VOLUME 2017, NUMBER 3

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 March and April 2017, CTU™ researchers identified lessons learned and observed notable developments in threat behaviors, the global threat landscape, and security trends:

- Criminal campaigns leveraging exploits disclosed by the Shadow Brokers group highlight the importance of vulnerability management processes and timely patching.
- A threat group created online social media profiles to build trust relationships with would-be victims.
- An advanced threat group targets the supply chains of large organizations as part of a global cyberespionage campaign.
- Quickly evicting threat actors from a compromised environment without a full understanding of their access can increase the scope and time of a comprehensive eviction.

Exploit disclosures highlight importance of timely patching

On April 9 and April 14, 2017, the Shadow Brokers group released archives of attack tools and information it claims originated from the U.S. National Security Agency (NSA). The tools leverage previously undisclosed Microsoft Windows and Oracle Solaris vulnerabilities and allow an attacker to gain control of vulnerable systems. However, CTU researchers determined that there were no functional exploits against fully patched and supported Microsoft software. Microsoft and Oracle addressed many of the vulnerabilities in security updates in March and April 2017.

Following the Shadow Brokers release, the CTU research team identified multiple threat campaigns scanning for vulnerable systems. On May 12, threat actors used one of the disclosed exploits to propagate WCry ransomware across a large number of unpatched or unsupported systems around the world, including a subset of systems owned by the UK's National Health Service. In response to this event, Microsoft took the unusual step of issuing security updates for unsupported Windows XP and Windows Server 2003 systems.

The release of these exploits and their subsequent use by threat actors reinforce the importance of identifying, prioritizing, and applying security updates in a timely fashion. CTU researchers also encourage organizations to remove or update legacy systems that are unsupported by the vendor. Systems that had Microsoft security updates applied prior to the WCry campaign were not impacted.

Threat group uses fake online personas

CTU researchers investigated a spearphishing campaign in March and April that used a malicious attachment to compromise systems. Investigation of further activity conducted by the same threat group revealed that the group established a fake social media persona to build trust relationships with targeted individuals. The threat group contacted the individual through social media and posed as a young woman with similar interests. Analysis of accounts linked to the fake persona indicated it had been active for more than a year and was likely used to target and facilitate malware delivery to individuals in several organizations.

This campaign illustrates the need for organizations to develop and maintain policies about employees' use of social media. Specific guidance may be appropriate for staff at high risk due to their profile or the nature of their role.

Cyberespionage group leverages managed service provider access

In April, the UK government reported a global cyberespionage campaign against managed service providers (MSPs) that handle IT infrastructure and services for large organizations. The adversary appears to leverage the trust relationships between MSPs and their customers as an access vector onto targeted networks.

CTU researchers refer to the threat group behind this campaign as BRONZE RIVERSIDE (also known as APT10 and MenuPass). BRONZE RIVERSIDE has been active since at least 2009 and is likely located in the People's Republic of China (PRC). It poses a significant threat to government, aerospace, defense, academic, pharmaceutical, and manufacturing organizations that produce intellectual property of value to the PRC. Organizations supporting these entities with managed IT infrastructure services are also targets.

Implementing processes and procedures for managing organizational risk in the supply chain can help mitigate these types of attacks. Organizations should identify their critical information assets and apply appropriate controls to protect them.

Credential-stealing phishing campaign uses spoofed CEO emails

CTU researchers tracked a phishing campaign in April that attempted to steal user credentials. The threat actor tailored emails to specific organizations, configuring the sender address to appear as if the email originated from each recipient's CEO. The message instructed recipients to open a malicious PDF attachment that linked to an attacker-controlled site where the victim was prompted to supply their credentials.

Threat actors continue to leverage publicly accessible information for tailoring phishing operations so the campaigns are more convincing and ultimately more successful. Organizations should educate personnel about phishing risks and implement a process that enables users to report suspicious emails to network defenders in a timely manner.

Failed evictions increase the cost of targeted intrusions

Compromised organizations often seek to evict attackers from their network as quickly as possible to minimize the damage. However, many persistent threat actors establish contingencies to access a compromised environment. Closing one entry point could cause the attacker to use another channel that the victim has not detected. Victims should balance the desire to evict quickly with the need to understand the full extent of the compromise to minimize the risk of re-entry.

SecureWorks incident responders assisted organizations in March and April following unsuccessful eviction attempts. In each case, the organizations isolated infected hosts and blocked command and control (C2) traffic before the environment had been fully assessed and instrumented. The threat actors used the following tactics to re-enter the affected networks, increasing the time and cost of a full eviction:

- Previously stolen credentials for remote access that only required single-factor (username and password) authentication
- Undetected malware on the system
- Other compromised hosts

Pre-emptive incident response planning can help reduce eviction times while increasing the chances of successful threat removal. Organizations should incorporate the following factors into the preparation process:

- Develop and document an effective targeted-intrusion incident-response plan.
- Deploy advanced endpoint threat detection services to detect malicious activity and understand threat actors' behavior, minimizing response and eviction times.
- Implement two-factor authentication for access to remote access solutions. This security control limits threat actors' ability to use stolen credentials from outside the network.

Conclusion

As sophisticated attacks increase and threat actors demonstrate greater adaptability, CTU researchers encourage organizations to consider the lessons learned from these incidents when planning and prioritizing cybersecurity strategies and operations. Implementing security best practices could limit the likelihood and impact of many intrusions, and understanding and addressing threat behaviors could help organizations anticipate and disrupt breaches and security incidents.

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