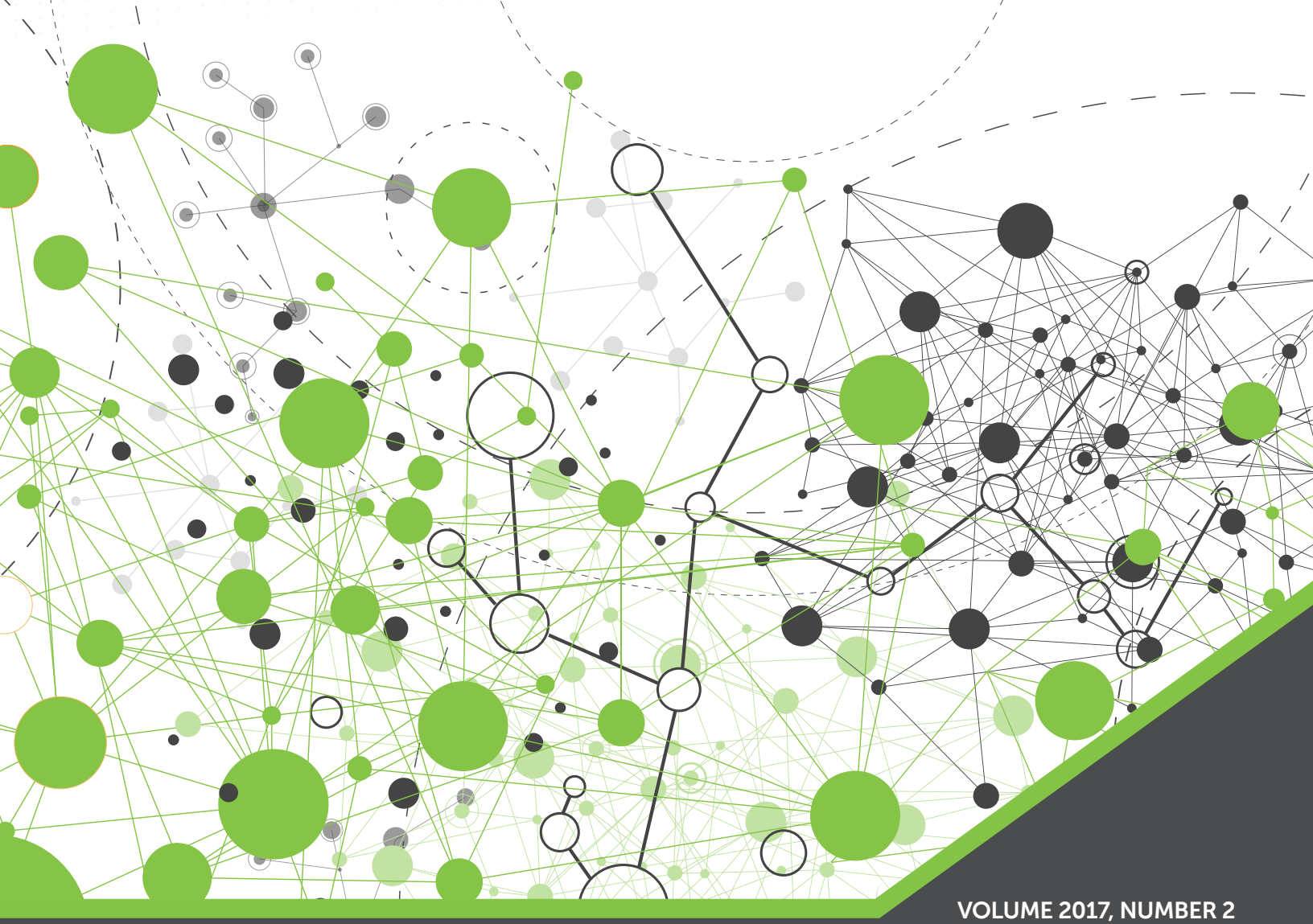


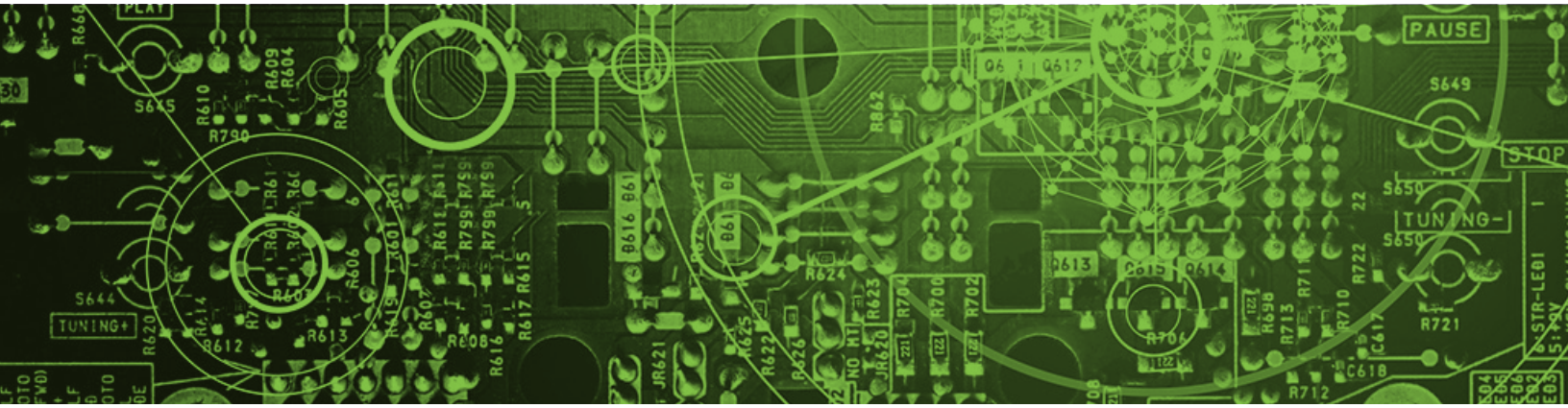
VOLUME 2017, NUMBER 2

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

- The NICKEL GLADSTONE threat group continued its trend of targeting financial networks for monetary gain.
- The Iranian COBALT GYPSY threat group used shortened phishing links and Microsoft Word macros to target Middle Eastern organizations in multiple verticals.
- The presence of three active threat groups on a single supplier's network demonstrated third-party risks.
- Limiting availability of native operating system administrative tools mitigates threat actors' capabilities.

High-impact targeted campaigns illustrate strategic web compromise risks

In early 2017, SecureWorks analysts tracked multiple large-scale targeted campaigns that used strategic web compromise (SWC) to deliver malware to victims. This methodology accounted for 16% of intrusion behavior observed during SecureWorks incident response (IR) engagements in 2016, representing a significant and ongoing risk for security teams to address. Testing, patching, and updating critical systems (including users' devices) are effective measures to guard against this threat. Endpoint instrumentation that detects exploitation attempts, such as Advanced Endpoint Threat Detection (AETD) - Red Cloak™, and network security technologies that use sandboxing methods to detonate suspicious files can help network defenders detect and respond to SWC threats.

Targeted threat group seeks to profit from financial networks

In February, an SWC of a Polish financial regulator's website redirected visitors from global banking organizations to attacker-controlled exploit sites that delivered malware. CTU researchers linked several characteristics of the malware to tools used by the NICKEL GLADSTONE threat group, which is likely associated with the North Korean government.

NICKEL GLADSTONE previously targeted other financial networks. In 2016, CTU researchers discovered evidence that it had compromised several banking networks in Asia and then used this access to initiate fraudulent Society for Worldwide Interbank Financial Telecommunication (SWIFT) transactions. Information identified during analysis of these intrusions suggested that the threat group intended to defraud financial organizations since at least May 2015. CTU researchers assess that NICKEL GLADSTONE poses a credible and enduring threat to global banking networks. Organizations in the financial vertical should carefully consider this group's particular methods when making security decisions.

Middle Eastern organizations attacked by Iranian threat actors

In January 2017, CTU researchers investigated a campaign that targeted technology, government, financial, and energy organizations in several Middle Eastern countries, including Egypt and Saudi Arabia. If recipients of the spearphishing emails clicked the shortened links to an attacker-controlled domain, a themed Microsoft Word document was downloaded and opened on the victim's system. The document leveraged Word macro functionality to download the publicly available PupyRAT remote access trojan, which gave the threat actor control of the compromised system. CTU analysis indicates that the COBALT GYPSY threat group is involved in this campaign. CTU researchers assess it is highly likely that COBALT GYPSY is associated with Iranian government-directed cyber operations.

Although this campaign appears to target organizations operating in the Middle East, all organizations should educate personnel about the dangers of spearphishing and shortened links. Network administrators should also evaluate the risks associated with macros being enabled in commonly used software.

Compromises of managed service provider networks highlight third-party risks

When investigating recent incidents affecting managed service providers (MSPs) that deliver IT and data-storage services, SecureWorks analysts discovered evidence that various threat groups, including those of Chinese and Russian origin, had compromised and operated within the MSPs' networks for several years. The findings of the investigations indicated that the groups targeted the MSPs to gain access to information owned by specific clients. Organizations that use MSPs for data storage or hosting should work closely with the suppliers to collectively identify security risks and then define strategies and processes to mitigate the likelihood and impact of a compromise.

Application whitelisting should include native system tools

Application whitelisting can prevent malware from running on user endpoints, but it only focuses on preventing third-party software from executing. It is not effective when threat actors use capabilities that already exist within compromised environments (also known as 'living off the land') rather than relying on malware and customized hacking tools. Network defenders should extend their application whitelisting approach to include tools that are native to baseline operating system (OS) builds. For example, threat actors commonly exploit the following native OS tools:

- PowerShell is an administrative configuration utility installed by default on Windows 7, Windows Server 2008 R2, and later Windows releases. Since January 2016, CTU researchers have observed multiple threat actors using weaponized documents to leverage PowerShell post-compromise.
- PsExec is a legitimate tool used by system administrators to execute commands locally and on remote systems. CTU researchers regularly observe threat actors exploiting it during network intrusions to move laterally to adjacent systems.

Organizations should limit the availability of these tools like these to users with a business need, increase visibility and logging (such as enabling PowerShell logging, which is disabled by default on older Windows releases), and monitor suspicious usage (e.g., reviewing Windows event logs for PsExec activity).

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