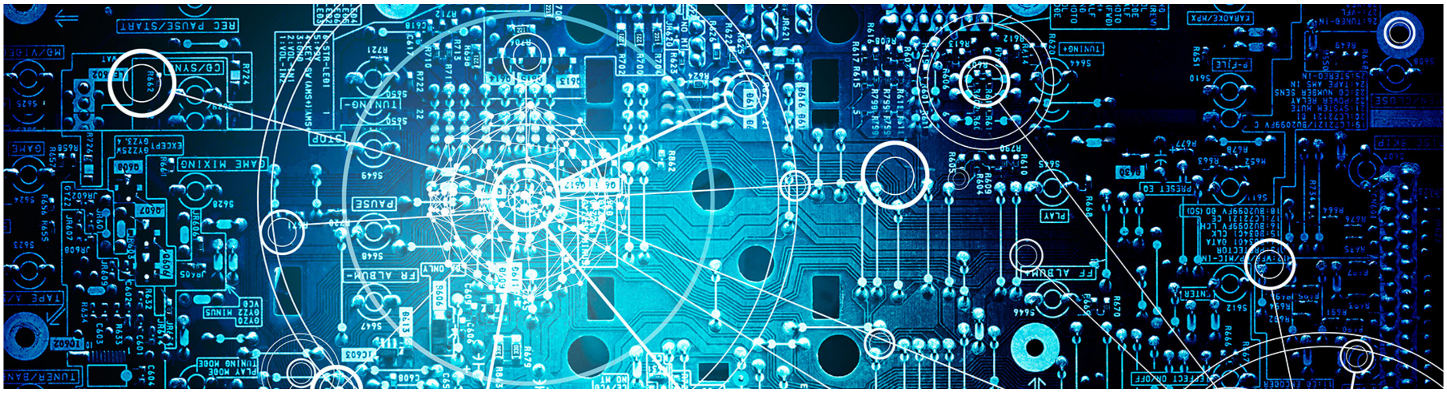
VOLUME 2017, NUMBER 1

# 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 November and December 2016, CTU™ researchers identified lessons learned and observed notable developments in threat behaviors and the global threat landscape:**

- ### Weak and outdated software enabled breaches

  Threat actors exploited a weak multi-factor authentication implementation and bypassed outdated antivirus software to breach organizations.

- ### Threat actors leveraged legitimate features

  To facilitate their activities in a compromised environment, threat actors used native system features rather than malware.

- ### Threat groups targeted organizations for espionage

  Government-sponsored threat groups updated their toolsets and conducted targeted espionage intrusions against networks in the technology, manufacturing, and defense verticals.

- ### Shamoon wiper malware reemerged

  Destructive malware reemerged that destroyed tens of thousands of devices in 2012.

## Threat actors overcame vulnerable two-factor authentication implementations

Two-factor authentication (2FA) requires users to provide two forms of identification; typically, something they know (i.e., a password) and something they have (i.e., a token). Tokens can be hard (e.g., an external hardware device) or soft (e.g., a software application that generates a passcode). Information security best practice often cites multi-factor authentication such as 2FA as an effective method for mitigating unauthorized access to data and systems.

During multiple breaches, SecureWorks incident responders observed threat groups circumventing 2FA by exploiting weaknesses in an organization's implementation. Threat actors leveraged remote access to staff email accounts protected by single-factor authentication to obtain soft tokens for network access. The extent of the activity carried out by the threat actors during these intrusions, which was partially enabled by the 2FA implementation flaws, resulted in complex and time-consuming incident response and remediation. The organizations could have mitigated this threat by implementing 2FA on remote email access and by requiring a hard token or a soft token from a non-networked device (e.g., a phone call).

## Antivirus and audit did not prevent credit card breach

In another incident, threat actors used the Adwind and NetWire remote access trojans (RATs) to compromise approximately 6,000 credit cards over a period of approximately 20 months. The affected systems were infected via phishing campaigns. The organization was running an outdated version of an antivirus product that would have identified and mitigated these threats, and a successful audit by an independent third party provided a false sense of security. Organizations should keep all software up to date and not mistake compliance audits for security assessments.

## Network intruders 'farmed the land' to evade detection

Threat actors often try to 'live off the land' in a compromised network environment, using available, legitimate tools and systems instead of installing malware. CTU researchers have observed an increase in 'farming the land' behavior, in which threat actors modify legitimate system tools to shape the victim's computing environment to their advantage. In one incident, threat actors used access to a compromised network to enable remote system management functionality. These remote management technologies allow a full range of configuration, data transfer, and remote execution capabilities over encrypted and unencrypted communication channels. The leveraged tools were not enabled by default on the compromised systems.

CTU researchers recommend checking if remote administration functionality such as PowerShell and Windows Remote Management (WinRM) are enabled. If they are and they have no legitimate purpose, the organization should disable the functionality and investigate how it was enabled. If there is a business need for these features, organizations should enable event logging to identify misuse. Endpoint monitoring can also detect threat actors using this functionality.

## U.S. agencies released joint report on Russian hacking

On December 29, the United States Department of Homeland Security (DHS) and the Federal Bureau of Investigation (FBI) released a joint analysis report on activity conducted by two Russian government-sponsored threat groups. CTU researchers refer to these groups as IRON TWILIGHT (formerly labeled by CTU researchers as TG-4127; also known as APT28 and Fancy Bear) and IRON HEMLOCK (also known as APT29 and The Dukes). The reported activity, named GRIZZLY STEPPE, involved targeting "the U.S. election, as well as a range of U.S. Government, political, and private sector entities."

CTU researchers have tracked IRON TWILIGHT activity since 2009 and IRON HEMLOCK activity since 2008, and have observed evidence supporting the connection to the Russian government. IRON TWILIGHT's capabilities include custom malware and exploit tools, a lateral expansion toolkit, and an email credential targeting system. IRON HEMLOCK leverages an array of highly capable and often custom cyberespionage tools. CTU researchers assess that IRON TWILIGHT poses the greater threat to more organizations due to its broad and unpredictable targeting strategy. IRON HEMLOCK focuses on targeting government and political networks, think tanks, and academic organizations.

## Destructive malware reemerged in Saudi Arabia

The destructive "Shamoon wiper" malware targeted six organizations located in Saudi Arabia in November. Four of the attacks resulted in significant data loss. Shamoon was first observed targeting the Middle East in 2012, when one impacted organization lost an estimated 30,000 endpoints. The attackers have not been identified, but threat groups could have various motives for targeting organizations in the Saudi Arabian government and energy verticals:

- Influence Saudi Arabian oil production policy
- Destabilize improved Western relations with Iran and the relaxation of Western sanctions
- Retaliate for Saudi Arabian involvement in conflicts in Syria and Yemen

Organizations could have detected the November attacks during multiple phases of the threat group's operation. The threat actors used similar malware and the same disk driver as the 2012 attacks, and the presence of hard-coded credentials within the samples analyzed by CTU researchers suggests the threat actors had access to the compromised network for a significant period of time prior to launching an attack. Endpoint monitoring technologies can block the execution of files based on a hash or other malware characteristics. An effective endpoint monitoring solution could also detect behaviors such as lateral movement within a network.

## Conclusion

Given these sophisticated attacks and increasingly adaptable threat actors, CTU researchers encourage organizations to consider the lessons learned from these incidents when designing their security protections. While implementing security best practices could limit the likelihood and impact of many intrusions, understanding and addressing threat behaviors can help organizations anticipate and disrupt potential breaches.

www.secureworks.com

# 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**
United Kingdom 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