Secureworks®

Threat Intelligence Executive Report

Volume 2018, Number 5

Presented by the Counter Threat Unit™ (CTU) research team

Executive Summary

The Secureworks® Counter Threat Unit™ (CTU) research team analyzes security threats and helps organizations protect their systems. During July and August 2018, CTU™ researchers identified lessons learned and observed notable developments in threat behaviors, the global threat landscape, and security trends:

- Universities were targeted by the COBALT DICKENS threat group.
- The United States government indicted IRON TWILIGHT threat actors for 2016 U.S. election hacking.
- BRONZE UNION targeted organizations with web shells.
- The GandCrab ransomware spread to new regions.

COBALT DICKENS targeted university credentials in large-scale campaign

In August 2018, CTU researchers discovered a website spoofing a login page for a university. The attackers hoped to harvest the credentials of victims who visited the fake page. Further research into the IP address hosting the spoofed page revealed a broader campaign to steal credentials. Forty domains contained 564 spoofed websites and login pages for 154 universities located in 14 countries, including Australia, Canada, China, Israel, Japan, Switzerland, Turkey, the United Kingdom, and the United States. After entering credentials into the fake login page, victims were redirected to the legitimate website, where they were automatically logged into a valid session or were prompted to enter their credentials again.

Organizations should incorporate multifactor authentication and implement complex password requirements.

The infrastructure for this campaign was similar to infrastructure used for cyber operations that CTU researchers attribute to the COBALT DICKENS threat group, which is associated with the Iranian government. In March 2018, the U.S. Department of Justice indicted the Mabna Institute and nine Iranian nationals in connection with COBALT DICKENS activity occurring between 2013 and 2017. However, the August activity suggests that the group continued its operations unabated. This widespread spoofing of login pages to steal credentials reinforces the need for organizations to incorporate multifactor authentication using secure protocols and to implement complex password requirements on publicly accessible systems.

IRON TWILIGHT threat actors indicted for 2016 U.S. election hacking

IRON TWILIGHT activity has persisted despite attributions and indictments.

On July 13, 2018, the United States Department of Justice (DOJ) announced the indictment of twelve Russian nationals for their involvement in cyber operations intended to interfere with the 2016 U.S. presidential election. The twelve individuals are members of the GRU, which is Russia's military intelligence service. According to the announcement, "in their official capacities, [the individuals] engaged in a sustained effort to hack into the computer networks of the Democratic Congressional Campaign Committee, the Democratic National Committee, and the presidential campaign of Hillary Clinton." The threat actors subsequently used online personas to dump information on the Internet with the intent of discrediting the Democratic campaign. CTU researchers observed and reported on the phishing activity referred to in the U.S. indictment in 2016, attributing the activity to the IRON TWILIGHT threat group.

On October 4, the DOJ, the UK National Cyber Security Centre (NCSC), and the Dutch Ministry of Defense issued press releases attributing a series of cyberattacks to the GRU. Several of the named individuals were also identified in the July 13 indictment. The October indictment also referenced other incidents that CTU researchers had previously attributed to the IRON TWILIGHT and IRON VIKING threat groups, such as attacks on Emmanuel Macron's political party during the 2017 French presidential elections and the 2016 compromise of World Anti-Doping Agency (WADA) systems. Despite these indictments and other public government and private-sector attributions of IRON TWILIGHT's activities to the Russian government, CTU researchers have no evidence that the threat group has moderated its activities.

BRONZE UNION continued to target vulnerable Internet servers

Restricting permissions can limit BRONZE UNION's ability to escalate privileges.

In mid-2018, CTU researchers became aware of a new web shell employed by the BRONZE UNION threat group. The threat actors used AbcShell to compromise Internet-facing systems and install additional malware and tools to entrench their position and harvest valuable credentials from compromised systems. The threat group has favored the use of web shells such as China Chopper and OwaAuth as a point of entry since at least 2013. AbcShell may represent the latest development effort from this threat group, as CTU researchers have not observed this web shell being used by other threat actors.

In one instance, BRONZE UNION deployed AbcShell to multiple Microsoft Exchange Servers, providing the threat actors with immediate access to several high-value systems and a perfect pivot point from which to further attack the victim's network. Timely patching and monitoring of high-risk systems are important defensive controls that can help defend against this ongoing threat. Restricting account permissions on Internet-facing systems can also limit opportunities for attackers to escalate their privileges when web shells are deployed.

GandCrab ransomware spread to new regions

In August 2018, CTU researchers observed malicious emails targeting Korean-language users. The emails were sent from a likely compromised account at Seoul-based manufacturer Kanghan Corp. The messages appeared to be targeting the Korbit South Korean Bitcoin exchange and the Hanmail South Korean email provider. The threat actors used a legal-themed lure that made allegations of improper conduct against the recipient. The email asked the recipient to respond to the attachment and "bring it with you at the time of interview." When opened, the malicious attachment delivered the GandCrab ransomware, which encrypted files on the victim's system and demanded a $1,200 USD ransom paid in cryptocurrency for recovery instructions.

GandCrab's business model makes it simultaneously available to many threat actors.

GandCrab is operated on a "ransomware-as-a-service" business model, meaning that many threat actors use it. The operators behind this ransomware continually develop the malware and add new features and language options. This incident involved GandCrab version 4, which targets English, German, Italian, Spanish, French, Korean, Japanese, and Chinese speaking regions.

Conclusion

These developments show that sophisticated threat actors are highly adaptable, and that public attribution by concerned governments may not be sufficient to disrupt or halt their operations. 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

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. Leveraging Secureworks' advanced security technologies and a network of industry contacts, the CTU research team tracks threat actors 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 clients 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® (NASDAQ: SCWX) is a leading global cybersecurity company that keeps organizations safe in a digitally connected world. By combining our visibility into threat behavior across client environments with our expertise and a powerful processing platform, we help organizations anticipate emerging threats, detect malicious activity in real time, assess risk, and take appropriate action to avoid or mitigate risk of a security breach. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™ www.secureworks.com

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
One Creechurch Place, 1 Creechurch Ln
London EC3A 5AY
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

