VOLUME 2017, NUMBER 5

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

- Use of social platforms to target victims necessitates a broader scope of social engineering training.
- Espionage campaigns against law firms underscored the need for a layered defense.
- Threat actors took advantage of gaps in business processes to steal funds.
- Phishing emails executed malicious code without user interaction.

Social engineering risks transcend corporate email

In July 2017, CTU researchers analyzed an espionage campaign targeting Middle Eastern organizations. The Iranian threat group used a fake persona named “Mia Ash” on multiple social platforms to establish relationships with targets and eventually send malware to steal victims’ credentials. Mia Ash’s social connections and the duration of the active profiles indicates that the social engineering aspect of this campaign was successful. The persona was active for nearly a year with more than 500 connections on LinkedIn and Facebook, most of which were probable COBALT GYPSY targets.

This campaign reinforces the need for continuous social engineering training that emphasizes interactions and information disclosure on non-corporate resources such as social media. Organizations should provide employees with instructions for reporting potential phishing messages received through corporate email, personal email, and social media platforms. Guidance should specifically address inquiries from an unknown third party regarding an employer, business systems, the corporate network, or requests such as opening a document or visiting a website.

Espionage campaign targeted legal vertical

CTU researchers analyzed a campaign targeting multiple law firms in which a threat actor exploited vulnerable third-party web applications to gain an initial foothold in the organization’s network. The attacker then ran malicious publicly available scripts that used online code-sharing repositories for command and control. Use of online repositories is a novel tactic that the CTU research team had not previously observed. The threat actors also deployed malware that leveraged DLL search order hijacking, which allows attackers to escalate privileges using legitimate programs. Legal firms are attractive targets for espionage attacks because they possess sensitive data and could provide an attack vector to their clients’ networks.

CTU researchers recommend that organizations review and monitor web applications for anomalous activity that could indicate attacks. Malicious commands could include SQL injection, so organizations should test Internet-facing applications for SQL injection vulnerabilities. Organizations should also restrict, monitor, and consider disabling PowerShell and other unused native tools on all systems. Clients of legal firms should review the security of sensitive data held on their behalf and assess the possibility that threat actors could abuse the trust between the two organizations.

Opportunistic criminals monetized nontechnical weaknesses

SecureWorks incident responders observed incidents that leveraged user trust and business process loopholes instead of malware or software vulnerabilities. In an incident that affected multiple organizations, threat actors used stolen credentials to access online payroll systems and then replaced employee bank account details with an attacker-controlled account. Affected organizations were only made aware after employees reported that personal details had changed or that they had not been paid. It is likely that the credentials used to access the payroll systems were stolen via phishing emails.

In another incident, an organization was notified that large amounts of personal employee data from its cloud-based human resources (HR) system was available for sale on underground forums. A SecureWorks forensic investigation concluded that the third party managing the HR system had been using default administrative credentials, which the threat actor accessed and used to generate reports containing employee data.

These incidents highlight the need for organizations to focus on more than technical security controls that detect and prevent malware. Opportunistic and targeted threat actors often use the path of least resistance and avoid malware if possible, so effective protection involves a combination of user education, established processes, and technical controls to manage system access. Two-factor authentication should always be used for sensitive and privileged systems. Organizations should also implement processes to monitor for unusual activity that accesses or modifies sensitive information.

Phishing emails automatically executed malicious code

CTU researchers observed a threat actor using Microsoft Outlook forms to deploy the Meterpreter post-exploitation tool to several systems in an already compromised network. Forms are Microsoft Outlook templates that define how the program presents and processes message information. There are default forms for a range of Outlook functions, including emails and meeting requests. Users can also create custom forms, which includes the ability to define custom Visual Basic Script (VBScript).

In this campaign, the threat actor used stolen credentials, likely obtained through previous credential-harvesting activity on the network, to deploy a malicious Outlook form to targeted accounts or systems. When the user received a phishing email that contained properties corresponding to this form, the form automatically retrieved the malicious content. In this incident, VBScript in the form retrieved the Meterpreter tool from a malicious domain.

Abusing Outlook forms provided a novel persistence mechanism that allowed the threat actor to regain access to the targeted network via an email that did not require user interaction. CTU researchers recommend that organizations implement multi-factor authentication to access Exchange servers and for Outlook accounts that have permissions to amend form libraries.

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 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