proofpoint.

TA410: The Group Behind LookBack Attacks Against U.S. Utilities Sector Returns with New Malware

JUNE 08, 2020 |

MICHAEL RAGGI, DENNIS SCHWARZ, AND GEORGI MLADENOV WITH THE PROOFPOINT THREAT RESEARCH TEAM

In August 2019, Proofpoint researchers **reported** that LookBack malware was targeting the United States (U.S.) utilities sector between July and August 2019. We then **continued** our analysis into additional LookBack campaigns that unfolded between August 21-29, 2019. These campaigns utilized malicious macro-laden documents in order to deliver modular malware to targeted utility providers across the U.S. At the same time as the LookBack campaigns, Proofpoint researchers identified a new, additional malware family named FlowCloud that was also being delivered to U.S. utilities providers.

FlowCloud malware, like LookBack, gives attackers complete control over a compromised system. Its remote access trojan (RAT) functionality includes the ability to access installed applications, the keyboard, mouse, screen, files, services, and processes with the ability to exfiltrate information via command and control.

We analyzed phishing campaigns between July-November 2019 and have determined that both LookBack and FlowCloud malware can be attributed to a single threat actor we are calling TA410. This conclusion is based on the threat actor's use of shared attachment macros, malware installation techniques, and overlapping delivery infrastructure.

In addition, our analysis found similarities between TA410 and TA429 (APT10) delivery tactics. Specifically, we have seen attachment macros that are common to both actors. TA410 campaigns detected in November 2019 included TA429 (APT10)-related infrastructure used in phishing attachment delivery macros. However, Proofpoint analysts believe that intentional reuse of well-publicized TA429 (APT10) techniques and infrastructure may be an attempt by threat actors to create a false flag. For this reason, while research is ongoing, we do not attribute LookBack and FlowCloud campaigns to TA429 (APT10). Proofpoint currently tracks TA429 (APT10) independently of TA410 campaigns.

Figure 1 below shows a timeline of the identified LookBack and FlowCloud campaigns.

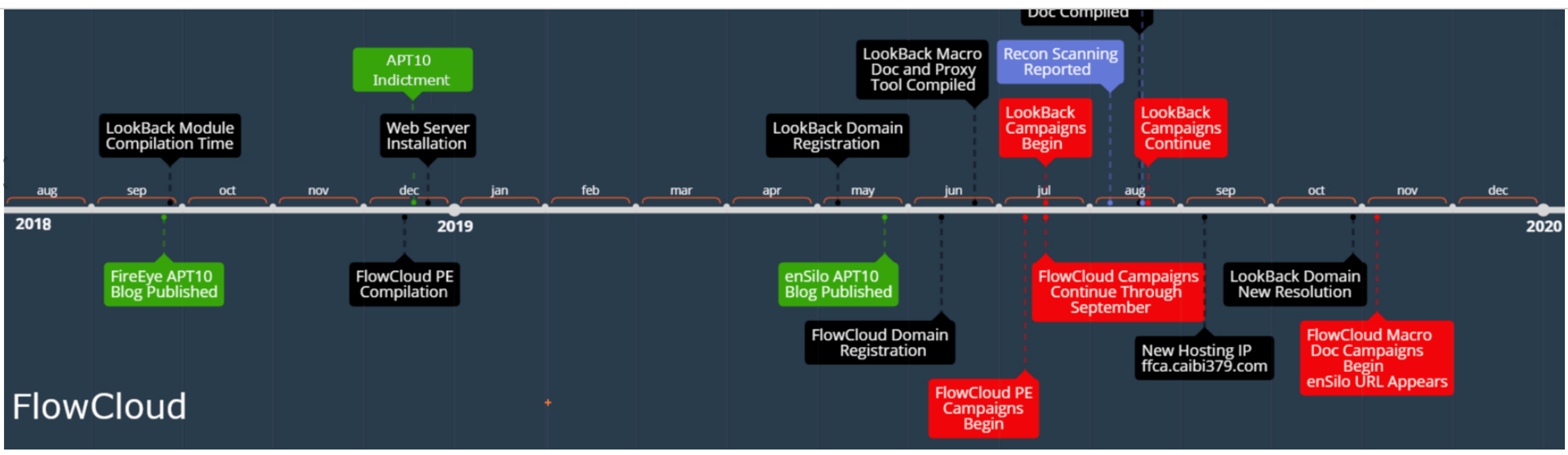

Figure 1 LookBack and FlowCloud Campaign Timeline

Delivery

Proofpoint researchers observed phishing campaigns beginning on July 10, 2019 that targeted utility providers across the United States with portable executable (PE) attachments and used subject lines such as “PowerSafe energy educational courses (30-days trial)”. These campaigns continued through September 2019.

Our analysis of these phishing campaigns determined that the PE attachments delivered a modular malware which the developers referred to in program data base (“PDB”) paths as “FlowCloud”. We therefore refer to these campaigns as “FlowCloud” based on the malware family they delivered. It’s notable that these FlowCloud campaigns were occurring at the same time as the LookBack campaigns that Proofpoint has previously documented. Both the FlowCloud and LookBack campaigns targeted utility providers in the United States. Both used training and certification-themed lures. And both used threat actor-controlled domains for delivery. In some cases, both FlowCloud and LookBack campaigns targeted not only the same companies but also the same recipients.

The senders of the emails that delivered FlowCloud malware utilized threat actor-controlled domains for delivery which impersonated energy sector training services, as well as utilized subdomains which contained the word “engineer”.

We observed a distinct change in FlowCloud delivery tactics beginning with attacks carried out in November 2019. The targeting of US utilities companies remained constant, but the threat actors shifted from PE attachments to malicious macro laden Microsoft Word documents that closely resembled the same delivery and installation macros used in LookBack malware campaigns.

Additionally, in November threat actors began to utilize the sender domain asce[.]email to deliver these attachments. This domain was first observed in June 2019 registered to the IP 103.253.41[.]75 which was used as a staging and reconnaissance IP in previous LookBack campaigns. On October 29, 2019, the domain resolved to the IP 134.209.99[.]169 which also hosted several energy certification and education themed domains. A number of these domains also shared an SSL certificate with delivery domains previously observed in the July and August 2019 FlowCloud phishing campaigns. The data from this SSL Certificate has been displayed in Figure 2. This figure demonstrates the actor’s use of a single SSL certificate for multiple energy and training themed domains. The actor listed the domains that were signed by the certificate in the Alternative Names field allowing for the identification of additional related infrastructure. A number of these domains were used in FlowCloud campaigns.

proofpoint.

Issued	2019-06-10
Expires	2019-09-08
Common Name	**powersafetrainings.org** (subject) **Let's Encrypt Authority X3** (issuer)
Alternative Names	**www.mails.energysemi.com** (subject) **powersafetraining.net** (subject) **powersafetrainings.org** (subject) **www.powersafetraining.net** (subject) **mails.energysemi.com** (subject) **www.powersafetrainings.org** (subject)
Organization Name	**Let's Encrypt** (issuer)
SSL Version	3
Organization Unit	
Street Address	
Locality	
State/Province	
Country	**US** (issuer)

118.25.97.43

Figure 2 Passive Total SSL Certificate data for powersafetrainings[.]org and related energy themed domains.

The table below shows the TA410 staging IPs, when they were first observed, the registered domains associated with them, and the malware delivered by emails originating from these domains.

IP	First Observed	Registered Domains	Malware Delivered
103.253.41[.]75	06/23/2019	***Delivery Domain:*** Nceess[.]com Globalenergycertification[.]com ***Registered Domain:*** Nerc[.]email Asce[.]email	LookBack
134.209.99[.]169	10/29/2019	***Delivery Domain:*** Asce[.]email ***Registered Domain:*** Powersafetraining[.]net ***Domains Related by SSL Certificate:*** mails.energysemi[.]com powersafetrainings[.]org www.mails.energysemi[.]com	FlowCloud

101.99.74[.]234	07/02/2019	***Delivery Domain*** www.powersafetrainings[.]org	FlowCloud

The content of the emails in the November 2019 campaigns impersonated the American Society of Civil Engineers and masqueraded as the legitimate domain asce[.]org. The structure of this email is very similar to the LookBack delivery emails constructed to impersonate the NCEES and Global Energy Certification in July 2019. Examples of the emails are included in Figure 3 and Figure 4.

Figure 3 ASCE-themed phishing email delivering FlowCloud malware November 2019

Figure 4 NCEES-themed phishing email delivering LookBack malware July 2019

Exploitation - Installation Macros

As noted above, after an extended period of using PE attachments to deliver FlowCloud in campaigns, the threat actors behind FlowCloud switched to using Microsoft Word documents with malicious macros at the beginning of November 2019. The Word document attachments and macros delivering FlowCloud had key similarities with the Word document attachments and macros we identified that delivered LookBack in July and August 2019.

Identical to the methodology used with LookBack, the FlowCloud macro used privacy enhanced mail (“.pem”) files which were subsequently renamed to the text file “pense1.txt”. This file is next saved as a portable executable file named “gup.exe” and executed using a version of the certutil.exe tool named “Temptcm.tmp”.

For comparison, Figure 5 November 2019 macro used to install FlowCloud malware shows the macro used to install FlowCloud while Figure 6 August 2019 macro used to install LookBack malware shows the macro used to install LookBack.

Figure 5 November 2019 macro used to install FlowCloud malware

Figure 6 August 2019 macro used to install LookBack malware

The “Exploitation” section in our blog **LookBack Malware Targets the United States Utilities Sector with Phishing Attacks Impersonating Engineering Licensing Boards** has a more in-depth explanation of this method used by LookBack. FlowCloud uses this same method exactly including identical macro concatenation code.

While we found the ultimate execution method for both the LookBack Gup proxy tool and FlowCloud malware were the same across both macro versions, we found that the FlowCloud macro introduced a new method for the delivery of the malware.

The earlier LookBack versions of the macro included the payload in numerous privacy enhanced email (“.pem”) files that were dropped when the attachment file is executed by the user. The FlowCloud version of the macro utilized a previously unobserved macro section to download the payload from a DropBox URL. Once the payload was downloaded, a FlowCloud malware PE in the form of a .pem file was saved as the variable “Pense1.txt”. Figure 7 FlowCloud Malware Macro delivery code shows the FlowCloud macro with the delivery section in question called out.

Figure 7 FlowCloud Malware Macro delivery code

The FlowCloud macro also contained a strange **try… catch** statement which initially attempts to download the FlowCloud payload from the DropBox URL as part of the try statement. However, if it was unable to retrieve the payload from that resource, a catch statement which was nearly identical to the try statement attempted to retrieve a malware resource from the URL http://ffca.caibi379[.]com/rwjh/qtinfo.txt”.”. Figure 8 FlowCloud Malware Catch statement macro code shows the **catch** statement in question.

Figure 8 FlowCloud Malware Catch statement macro code

This **try…catch** sequence is significant because the URL in the catch statement and malware resource was previously mentioned in a May 2019 blog by enSilo entitled “**Uncovering New Activity by APT10**”. The blog claims that this URL delivered a modified Quasar RAT payload which included the addition of SharpSploit, an opensource post-exploitation tool. When analyzed on the same date of FlowCloud campaign delivery this URL and resource was unavailable, while the DropBox URL successfully delivered the FlowCloud .pem file. While Proofpoint has not independently verified these attribution claims made by other researchers regarding the referenced Quasar RAT sample, the use of this URL represents a previously undisclosed overlap with publicly reported indicators of compromise attributed to TA429 (APT10). While on the surface this domain may imply links to TA429 (APT10), we have identified several aberrations regarding the domain registration information and inactive nature of the URL and will discuss them at length at length later in this blog.

FlowCloud Malware

Our analysis of the FlowCloud malware determined that it is a multi-stage payload comprised of a large code base written in C++. The code demonstrates a level of complexity including numerous components, extensive object-oriented programming, and use of legitimate and imitation QQ files for initial and later stage execution. We found further imitation of QQ components in several modules used throughout FlowCloud execution. The malware name “FlowCloud” was taken from distinctive PDB paths observed in numerous malware components. These values have been included in the IOCs section at the end of this blog.

FlowCloud malware is capable of RAT functionalities based on its available commands including accessing the clipboard, installed applications, keyboard, mouse, screen, files, services, and processes with the ability to exfiltrate information via command and control. Additionally, the malware variants analyzed have several distinct characteristics that indicate the malware may have been active in the threat landscape since at least July 2016.

years. Public **reports** around FlowCloud malware components and related installation directory paths suggest that versions of this malware may have been observed in the wild as early as July 2016. Additionally, development of this malware around legitimate QQ files and the identification of malware samples uploaded to VirusTotal from Japan in December 2018 and earlier this year from Taiwan indicate that the malware may have been active for some time in Asia prior to its appearance targeting the US utilities sector.

Figure 9 Flowchart of FlowCloud Loader Functionality below outlines FlowCloud's loader functionality.

Figure 9 Flowchart of FlowCloud Loader Functionality

- EhStorAuthn.exe extracts the subsequent payload file components and installs them to the directory C:\Windows\Media\SystemPCAXD\ado\fc. This file also sets registry key values that store the keylogger drivers and the malware configuration as the value “KEY_LOCAL_MACHINE\SYSTEM\Setup\PrintResponsor\<2-4>”.

- EhStorAuthn.exe is a legitimate portable executable file used by QQ with the initial name QQSetupEx.exe. This file is used to load the file dlcore.dll as part of its natural downloader routine.

- Dlcore.dll is a DLL crafted by the threat actors that functions as a shellcode injector pulling the shellcode from a file named rebare.dat. This file imitates a legitimate QQ component.
  When the shellcode within rebare.dat is executed it in turn executes a RAT installer file named rescure.dat.

- Rescure.dat is an XOR encrypted DLL file that installs the RAT based application responsor.dat which installs the keylogger driver and manages the RAT functionality.

- Responsor.dat unpacks several modules (rescure86.dat or rescure64.dat) to the registry %TEMP%\{0d47c9bc-7b04-4d81-9ad8-b2e00681de8e}" and installs the unpacked file as a service named “FSFilter Activity Monitor” or “FltMgr”.

- Finally, Responsor.dat starts the RAT when the rescure.dat function “startModule” is called.

- Several legitimate Microsoft Windows files were also used by the malware for thread injection.

- EhStorAuthn_shadow.exe (hhw.exe) a Microsoft HTML Help Workshop file was used as a placeholder for thread injection.

- Hha.dll is a component of Microsoft HTML Help Workshop and is required to run EhStorAuthn_shadow.exe.

The malware stores its configuration in the registry alongside drivers utilized by the malware’s keylogger components. Several additional distinct registry keys are generated which indicate the malware’s current execution stage on the host. Some of these keys are included in the table below.

Registry Key	Originating Component	Description
HKEY_LOCAL_MACHINE\SYSTEM\Setup\PrintResponsor\2	Gup.exe	32bit Driver, Keylogger
HKEY_LOCAL_MACHINE\SYSTEM\Setup\PrintResponsor\3	Gup.exe	64bit Driver, Keylogger
HKEY_LOCAL_MACHINE\SYSTEM\Setup\PrintResponsor\4	Gup.exe	RAT config
HKEY_LOCAL_MACHINE\HARDWARE\{2DB80286-1784-48b5-A751-B6ED1F490303}	Dlcore.dll	Execution Stage Executing dlcore.dll
HKEY_LOCAL_MACHINE\HARDWARE\{804423C2-F490-4ac3-BFA5-13DEDE63A71A}	rescure.dat	Execution Stage Install keylogger driver
HKEY_LOCAL_MACHINE\HARDWARE\{A5124AF5-DF23-49bf-B0ED-A18ED3DEA027}	rescure.dat	Execution Stage RAT fully installed.

FlowCloud Configuration

The FlowCloud loader component EhStorAuthn.exe stores the malware configuration in the registry early in the installation chain and is represented in the table above. The Registry data is composed of multiple encrypted headers (using XORs and RORs) and data is encrypted using a modified (or broken) AES algorithm. The plaintext data is compressed with ZLIB and

Figure 10 Example of a configuration as displayed by debug logging

Command and Control

FlowCloud malware handles configuration updates, file exfiltration, and commands as independent threads utilizing a custom binary C2 protocol. We identified these independent threads as part of an extensive command handling functionality with distinct command managers existing for each command. The sample we analyzed utilized port 55555 for file exfiltration and port 55556 for all other data. We identified FlowCloud communication with the IP 188.131.233[.]27. The requests and responses are composed of multiple encrypted headers (using XORs and RORs) and TEA encrypted data using a key generation scheme involving a hardcoded string of random characters and MD5 hashing. The plaintext data is compressed using ZLIB and serialized using Google's Protocol Buffers. An example parsing of an initial beacon is demonstrated in Figure 11 Example of FlowCloud parsing an initial C2 beacon:

Figure 11 Example of FlowCloud parsing an initial C2 beacon

Comparing Public TA429 (APT10) Indicators with TA410 Campaigns

Publications by **FireEye** and EnSilo regarding TA429 (APT10) campaigns contain indicators that later appeared in TA410 campaigns. In our retrospective analysis of that research, we determined that TA429 (APT10) used phishing macros that were later seen being used by LookBack and FlowCloud malware. Additionally, we identified the Quasar RAT delivery URL hxxp://ffca.caibi379[.]com/rwjh/qtinfo.txt used by FlowCloud macros in November, which was published in the enSilo report prior to observable weaponization for TA410 campaigns.

Interestingly, the compilation date of several LookBack malware modules used in July 2019 were September 14, 2018. This includes the SodomMain and SodomNormal modules covered in previous Proofpoint blogs on LookBack malware. That date is just one day after FireEye released their initial analysis of similar TA429 (APT10) macros utilized in Japan on September 13, 2018.

While LookBack malware samples were not observed in the wild until June 2019, this September 2018 compilation date demonstrates a large lag time between compilation and delivery. This possibly suggests manipulation of compilation times by threat actors but has not been conclusively determined.

The first identified server installation by TA410 on actor-controlled infrastructure occurred in December 2018. Most of the domain registration (weaponization) for LookBack and FlowCloud campaigns began in May and June 2019 respectively. These events were after FireEye's initial publication in September 2018.

indicate that the registrant email and address fields for the domain were updated on June 7, 2019. The A record for the domain was updated on September 9, 2019 at which time it resolved to the IP 34.80.27[.]200 contained within an ASN owned by Google. For the prior eight months beginning on January 2, 2019 and encompassing the period of activity discussed by enSilo, the domain was hosted on several IP's in an ASN owned by APNIC Hostmaster. The shift away from IP infrastructure owned by APNIC represents a departure in threat actor infrastructure hosting tactics well after the publication by enSilo and within the weaponization period for TA410's campaign targeting US utilities. While this research is not conclusive, it demonstrates that all observed TA429 (APT10) similarities and indicators of compromise were available publicly prior to the start of TA410 campaigns. Therefore, while not conclusive from current analysis, the possibility remains that these overlaps represent false flag activity by the TA410 threat actor. Based on this analysis Proofpoint analysts track TA410 as a distinct threat actor from TA429 (APT10) at this time.

Conclusion

The convergence of LookBack and FlowCloud malware campaigns in November 2019 demonstrates the capabilities of TA410 actors to distinctly utilize multiple tools as part of a single ongoing campaign against US utilities providers. Both malware families demonstrate a level of sophistication in their conception and development while the extensible code base of FlowCloud malware suggests that this group may have been operating as early as 2016. TA410 operators demonstrate a willingness to dynamically evolve phishing tactics to increase the effectiveness of their campaigns and a keen eye towards plausible social engineering within a very select targeted sector. It remains unclear if the nature of the tactics and indicators that are shared with TA429 (APT10) were developed by this group or culled from readily available technical reporting that pre-dated these campaigns. The possibility remains that these overlaps represent intentional false flag efforts to cloak the identity of these perpetrators while they targeted a critical and geo-politically sensitive sector of energy providers in the US. Regardless of the actor's intention, TA410 has established itself as a motivated actor with mature toolsets carrying out long term campaigns against highly important and geographically concentrated target sets.

Indicators of Compromise (IOCs)

IOC	IOC Type	Description
faa80e0692ba120e38924ccd46f6be3c25b8edf7cddaa8960fe9ea632dc4a045	SHA256	PE Attachment - our infrastructure offer annÃ¢Â€Â®cod.exe
b7960d1f40b727bbea18a0e5c62bafcb54c9ec73be3e69e787b7ddafd2aae364	SHA256	PE Attachment - powersafe courses annÃ¢Â€Â®cod.exe
26eb8a1f0bdde626601d039ea0f2c92a7921152371bafe5e811c6a1831f071ce	SHA256	FlowCloud MS Word Macro Attachment - personal invitation.doc
cd8f877c9a1c31179b633fd74bd5050e4d48eda29244230348c6f84878d0c33c	SHA256	Dropped Files - Cert.pem
e4ad5d3213425c58778d8a0244df4cd99c748f58852d8ac71b46326efd5b3220	SHA256	Dropped Files - pense1.txt
589229e2bd93100049909edf9825dce24ff963a0c465d969027db34e2eb878b4	SHA256	Dropped Files - Temptcm.tmp
1334c742f2aec7e8412d76ba228b99935a49dc96a1e8e1f3446d9f61247ae47e	SHA256	Dropped Files - EhStorAuthn.exe
de30929ef958211f9315e27a7aa45ef061726a76990ddc6b9d9f189b9fbdd45a	SHA256	Dropped Files - dlcore.dll
0b013ccd9e10d7589994629aed18ffe2388cbd745b5b28ab39c07835295a1ca9	SHA256	Dropped Files - rebare.dat

proofpoint.

d5191327a984fab990bfb0e811688e65e9aaa751c3d93fa92487e8a95cb2eea8	SHA256	Dropped Files - responsor.dat
0701cc7eb1af616294e90cbb35c99fa2b29d2aada9fcbdcdaf578b3fcf9b56c7	SHA256	Dropped Files - EhStorAuthn_shadow.exe
27f5df1d35744cf283702fce384ce8cfb2f240bae5d725335ca1b90d6128bd40	SHA256	Dropped Files - rescure64.dat
13e761f459c87c921dfb985cbc6489060eb86b4200c4dd99692d6936de8df5ba	SHA256	Dropped Files - rescure86.dat
2481fd08abac0bfefe8d8b1fa3beb70f8f9424a1601aa08e195c0c14e1547c27	SHA256	Dropped Files - hha.dll
188.131.233[.]27	IP	C&C IP
118.25.97[.]43	IP	Sender IP
34.80.27[.]200	IP	Sender IP
134.209.99[.]169	IP	Staging IP
101.99.74[.]234	IP	Staging IP
Asce[.]email	Domain	Phishing Domain
powersafetrainings[.]org	Domain	Phishing Domain
mails.daveengineer[.]com	Domain	Phishing Domain
powersafetraining[.]net	Domain	Related Infrastructure
mails.energysemi[.]com	Domain	Related Infrastructure
www.mails.energysemi[.]com	Domain	Related Infrastructure
www.powersafetraining[.]net	Domain	Related Infrastructure
www.powersafetrainings[.]org	Domain	Related Infrastructure
ffca.caibi379[.]com	Domain	Macro Domain
http://ffca.caibi379[.]com/rwjh/qtinfo.txt	URL	FlowCloud Macro Delivery URL Inactive
https://www.dropbox[.]com:443/s/ddgifm4ityqwx60/Cert.pem?dl=1	URL	FlowCloud Macro Delivery URL
HKEY_LOCAL_MACHINE\SYSTEM\Setup\PrintResponsor\2	Registry Key	FlowCloud Registry Key
HKEY_LOCAL_MACHINE\SYSTEM\Setup\PrintResponsor\3	Registry Key	FlowCloud Registry Key
HKEY_LOCAL_MACHINE\SYSTEM\Setup\PrintResponsor\4	Registry Key	FlowCloud Registry Key

HKEY_LOCAL_MACHINE\HARDWARE\{804423C2-F490-4ac3-BFA5-13DEDE63A71A}	Registry Key	FlowCloud Registry Key
HKEY_LOCAL_MACHINE\HARDWARE\{A5124AF5-DF23-49bf-B0ED-A18ED3DEA027}	Registry Key	FlowCloud Registry Key
G:\FlowCloud\trunk\Dev\src\fcClient\Release\QQSetupEx_func.pdb	File Path	FlowCloud PDB Path
g:\FlowCloud\trunk\Dev\src\fcClient\Release\fcClientDll.pdb	File Path	FlowCloud PDB Path
F:\FlowCloud\trunk\Dev\src\fcClient\kmspy\Driver\Release\Driver.pdb	File Path	FlowCloud PDB Path
F:\FlowCloud\trunk\Dev\src\fcClient\kmspy\Driver\x64\Release\Driver.pdb	File Path	FlowCloud PDB Path

ET and ETPRO Suricata/SNORT Signatures

2837783 ETPRO TROJAN Win32/LookBack CnC Activity

← Previous Blog Post

Next Blog Post →

proofpoint.

Products

Protect People

Defend Data

Mitigate Human Risk

Premium Services

Get Support

Product Support Login

Support Services

IP Address Blocked?

Connect with Us

+1-408-517-4710

Attend an Event

Contact Us

Free Demo Request

More

About Proofpoint

Why Proofpoint

Careers

Leadership Team

News Center

Privacy and Trust