accenture

Steal(Bit) or exfil, what does it (Ex)Matter? Comparative Analysis of Custom Exfiltration Tools

Executive Summary

In the proliferation of Ransomware as a Service (RaaS) operations as showcased by our previous blog, "Diving into double extortion campaigns", tools to aid data exfiltration tactics have become a commodity. In addition to using ubiquitous tools such as Rclone, MegaSync, and FileZilla, ransomware and extortion groups have crafted custom exfiltration tools tailored to their operations. The continued use and development of these custom tools is a testament to their success, often simplifying and accelerating data exfiltration.

In this blog, we will examine two (2) exfiltration toolsets identified during CIFR incident response engagements conducted between the fourth quarter of 2021 and the first quarter of 2022: StealBit and ExMatter. We will provide a comparative and temporal analysis of the tools and the ongoing utilization and development efforts observed over time.

- Discovered in 2021, StealBit and ExMatter are custom exfiltration tools that were originally known to be utilized by LockBit and BlackMatter ransomware operations, respectively.
- A testament to their functionality and effectiveness, these tools have gained popularity across the ransomware and extortion ecosystem.
- Since their original discovery, Accenture Security has observed modified versions of the tools utilized in multiple ransomware incidents involving BlackCat (aka ALPHV) and LockBit operators, as well as recent adoption by Conti operators, from the fourth quarter of 2021 and the first quarter of 2022.
- Based on comparative analysis of the tools, while data exfiltration is the consistent operational objective, the path to achieve that objective and the supporting functionality of each exfiltration tool varies slightly based on configuration, implementation details, and the operational environment. These variations can create challenges for network defenders.
- Furthermore, based on analysis of more than 15 samples, ExMatter adopts a more targeted approach to file discovery and exfiltration, while StealBit casts a wider net, especially for newer versions with geolocation restrictions removed.
- Of note, a modified version of ExMatter discovered in the first quarter of 2022 includes targeting of Computer Assisted Design (CAD) files, which suggests the operators are interested in exfiltrating data related to engineering documents or product designs that are common in industrial environments across the automotive, aviation, and manufacturing sectors.
- Based on analysis of samples obtained from various collection sources, Accenture Security assesses with high confidence that the tools are being continuously developed and improved upon by their authors, and utilization of the tools will continue into the second quarter of 2022 and beyond.

⇒ Skip ahead to Q1 2022 Intrusion Analysis Insights
⇒ Skip ahead to Comparative Analysis – Summary
⇒ Skip ahead to Network Infrastructure Trends
⇒ Skip ahead to tactical analysis of StealBit & ExMatter
⇒ Skip ahead to Countermeasures and Detection Opportunities
⇒ Skip ahead to MITRE ATT&ACK TTPs

Q1 2022 Intrusion Analysis Insights

Symantec first publicly described **ExMatter** in November 2021 and connected the tool with at least one affiliate using the BlackMatter ransomware variant at the time. The presence of a modified version of ExMatter (aka Fendr) was revealed through investigations conducted by Accenture Security during several distinct ransomware incidents. Between the fourth quarter of 2021 and the first quarter of 2022, CIFR incident responders identified BlackMatter and BlackCat ransomware operators using various versions of the tool to aide exfiltration operations, as well as Conti ransomware operators during the same time period.

LockBit, formerly known as ABCD ransomware, was first launched in September 2019. However, it was not until LockBit's v2.0 release in June 2021 that the group developed and utilized the **StealBit** exfiltration tool in its operations.

During a recent investigation involving the LockBit v2.0 ransomware, Accenture Security discovered that the operators initially attempted to download StealBit from a remote server, but ultimately pivoted to the open-source utility Rclone as attempts to utilize the tool were prevented. This data point is a testament to the group's versatility as it shows that while the LockBit operators may prefer to use their custom tools, they will ultimately adopt a path of least resistance to achieve their objectives. Furthermore, development efforts for StealBit might have slowed as the more recent compiled versions observed were from the fourth quarter of 2021, which included updates for broader targeting through removal of geolocation restrictions, as well as the removal of creation time-date-stamp.

Industries impacted include the financial services, retail, professional services, and energy sectors, with victims across North America, Europe, and Australia.

Accenture Security assesses with high confidence that the tools are being continuously developed and improved upon by their authors as the more recent samples analyzed include additional features and options for customization. For example, a recent version of ExMatter analyzed during an incident response engagement included specific targeting of CAD files, which suggests the operators may be interested in exfiltrating sensitive intellectual property related to engineering documents or product designs that are common in industrial environments such as the automotive, aviation, and manufacturing sectors.

Technical Analysis – Comparing StealBit and ExMatter

Both custom exfiltration tools are designed to work on a 32-bit Windows system (Intel 386 or later). Each tool also includes obfuscation techniques that can mask certain data, or code. Important information such as network information of the command-and-control (C2) server

address is encrypted in StealBit, while variants of ExMatter's code are protected and obfuscated using ConfuserEx (a free, open-source, .NET code protector), and Themida.

StealBit and ExMatter Comparison Summary

	StealBit	ExMatter
File Type	Win32 EXE.	Win32 EXE (.NET).
Operating System	Windows Vista and later versions.	Windows XP and later versions.
Targeting Approach	Targets all files except specific blacklisted items. Avoids common system files and programs.	Targets specific sets of files based on defined criteria. Avoids common system files and programs.
Obfuscation	Data encrypted with Rivest Cipher 4 (RC4) and XOR.	Code is Protected by ConfuserEx, with some less-prevalent variants utilizing other options.
Usage Flexibility	Accepts specific command-line parameters.	Accepts specific command-line parameters.
Network	Uses HTTP PUT method for exfiltration. C2 infrastructure identified during analysis is hosted by nine (9) unique hosting services / ASNs.	Uses secure file transfer protocol (SFTP), SOCKS5, or WebDAV for exfiltration. C2 infrastructure identified during analysis is hosted across two (2) unique hosting services / ASNs, with over 85% hosted by one (1) provider / ASN.

Table 1 – Tool Comparison Summary

Network Infrastructure Trends

During analysis of ExMatter and StealBit, Accenture Security identified the details of C2 servers used for exfiltration. The IP addresses for the C2 infrastructure were hard coded in each variant analyzed and might be statically encrypted or visible on its configuration. Based our analysis, Digital Ocean hosts twelve (12) of the fourteen (14) IP addresses, while Linode host the other two (2) present in ExMatter samples that were analyzed. However, the IP addresses observed to be connected to StealBit are hosted by several different hosting providers, suggesting a higher degree of operational obfuscation.

Accenture Security partnered with DigitialOcean's Security Team to evaluate the identified C2 infrastructure below. According to DigitalOcean, given the propensity for C2 infrastructure to run on public cloud, DigitalOcean's Security Team takes an aggressive approach toward mitigating harm and protecting potential victims from compromise in collaboration with the Critical Infrastructure Security Agency (CISA).

IP Address	Hosting Provider
104.248.142.137	Digital Ocean
134.122.108.252	Digital Ocean
138.197.183.62	Digital Ocean
142.93.108.213	Digital Ocean
188.166.211.227	Digital Ocean
64.227.70.115	Digital Ocean
68.183.208.242	Digital Ocean
157.230.28.192	Digital Ocean
159.89.128.13	Digital Ocean
165.22.84.147	Digital Ocean
164.92.229.32	Digital Ocean
164.92.232.192	Digital Ocean
104.237.130.71	Linode
172.105.111.15	Linode

Table 2 – ExMatter-related IPs

IP Address	Hosting Provider
88.80.147.102	Belcloud
139.60.160.200	Hostkey
45.227.255.190	Okpay Investment Company
193.162.143.218	FirstByte
193.38.235.234	VDSina
185.215.113.39	1337Team Limited
168.100.11.72	BL Networks
185.182.193.120	WorldStream
93.190.143.101	WorldStream
174.138.62.35	Digital Ocean

Table 3 – StealBit-related IPs

Tactical Comparison

StealBit and **ExMatter** both primarily use five primary MITRE ATT&CK tactics crucial to fulfil the operator's ultimate objectives –Execution, Defense Evasion, Discovery, Collection, and Exfiltration.

1.0 Execution

StealBit uses native APIs on various parts of its execution, specifically the Rtl, and Nt/Zw versions of the native system services routines, for optimization purposes. Moreover, it heavily utilizes inter-process communication through the creation and utilization of a named pipe "STEALBIT-MASTER-PIPE". This enables multiple instances to run and communicate with one another, showcasing its scaling capability.

Likewise, **ExMatter**, uses a native API, such as RtlGetVersion to get the OS version number. Its routine also includes several Windows APIs contained in the NativeMethods class of the AlphaFS (Alphaleonis) .NET library it uses. AlphaFS provides Win32 file system functionality similar to System.IO, but with additional support for advanced NTFS features.

2.0 Defense Evasion

StealBit and ExMatter both use the same set of techniques to bolster their defense evasion capability. The first technique is to hide windows and conceal malicious activities from their victims.

To achieve this, **StealBit** registers the **F2** hotkey which it will use to hide its graphical user interface (GUI). Newer versions accept the parameters -hide/-, yes/y, no/n to control the visibility of its GUI window.

StealBit also bolstered its defense evasion capability through the detection and avoidance of debuggers. It performs a check whether it is being debugged or not through checking the NtGlobalFlag from the Process Environment Block (PEB). When a process is being debugged, the NtGlobalFlag is set to 0x70, the sum of FLG_HEAP_ENABLE_TAIL_CHECK(0x10), FLG_HEAP_ENABLE_FREE_CHECK (0x20), and FLG_HEAP_VALIDATE_PARAMETERS (0x40). Once it detects that it is loaded by a debugger, the process will be trapped in a loop.

Upon execution of **ExMatter** with parameter nowmd or -nownd, it will attempt to hide its own window using the ShowWindow function.

```
ShowWindow(Process.GetCurrentProcess().MainWindowHandle, 0);
```

Additionally, both toolsets attempt to remove traces of their executables when they are finished executing. Newer versions of StealBit can accept the parameter -delete/-d to perform self-deletion through the command “del /f /q <file path of StealBit executable>”.

ExMatter can "melt" or perform self-deletion through PowerShell Scripting following execution.

```
"C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"  -WindowStyle
Hidden -C $path = 'C:\Users\user\Desktop\sender2.exe';Get-Process | Where-
Object {$_.Path -like $path} | Stop-Process -Force;[byte[]]$arr = new-
object byte[] 65536;Set-Content -Path $path -Value $arr;Remove-Item -Path
$path;
```

Furthermore, to make detection and analysis difficult, StealBit uses RC4-encrypted strings for its operations, and an XOR encrypted configuration file that contains a unique identifier and five (5) IP addresses to which it will exfiltrate the stolen file contents to.

```
0040E250 00 00 00 00 00 00 00 00 4C 43 50 41 30 00 38 38 ........LCPA0.88
0040E260 2E 38 30 2E 31 34 37 2E 31 30 32 00 00 00 00 00 .80.147.102.....
0040E270 00 00 00 00 31 36 38 2E 31 30 30 2E 31 31 2E 37 ....168.100.11.7
0040E280 32 00 00 00 00 00 00 00 00 00 31 33 39 2E 36 30 2.........139.60
0040E290 2E 31 36 30 2E 32 30 30 00 00 00 00 00 00 00 00 .160.200........
0040E2A0 31 39 33 2E 33 38 2E 32 33 35 2E 32 33 34 00 00 193.38.235.234..
0040E2B0 00 00 00 00 00 00 31 37 34 2E 31 33 38 2E 36 32 ......174.138.62
0040E2C0 2E 33 35 00 00 00 00 00 00 00 00 00 0D 00 00 00 .35.............
```

Image 1 – Decrypted Network Information from StealBit

While some variants of ExMatter are obfuscated through ConfuserEx, a free and open-source .NET code protector, there are few variants that also utilize Themida, VMProtect, or ILProtector.

3.0 Discovery

As an essential tactic for exfiltration, both StealBit and ExMatter perform file and directory discovery and system information discovery.

StealBit traverses the file system of the infected computer, enumerating files and subdirectories (through the FindFirstFile and FindNextFile APIs) starting from the target path. It checks the OS Major Version in preparation for console window implementation. It also gathers the system's local time, domain name (if any), and hostname to be displayed in the GUI. The domain name and hostname gathered will also be sent to its C2 server during exfiltration.

ExMatter retrieves the drive names of all logical drives on the infected computer and checks all file path names. It will then search for files last modified during a specific period:

- Files modified in the last six months
- Files modified between one and six years ago
    - (Possibly due to code error, this will not execute)
- Files modified during the execution of the tool
    - (time = now)

It collects the infected system's domain name and hostname, which are used as part of staging preparation for exfiltration.

A major difference between the two is StealBit's use of geolocation checking. Older versions of StealBit identifies the victim's location based on their default system language. If determined to be running a language associated with these locations, the variant will not execute if the location of the victim is from any of the countries listed below. Newer versions of StealBit analyzed do not include these restrictions, suggesting a change in tactics by the operators:

- Azerbaijan
- Armenia
- Belarus
- Georgia
- Kazakhstan
- Kyrgyzstan
- Moldova
- Russia
- Tajikistan
- Turkmenistan
- Uzbekistan
- Ukraine

4.0 Collection

Each exfiltration tool has specific target file criteria for samples to collect from, as well as a set of conditions to avoid.

StealBit accepts a file path or directory path as a parameter, which will be used as the target of its exfiltration routine. If the parameter is a file, it will exfiltrate the content of the file. If the parameter is a directory, it will exfiltrate the content of the files stored at the given directory. The GUI also supports dragging and dropping as a method for files to be collected.

It only collects files that match the following criteria:

- File size less than or equal to .54 GB.
- File must not have a system attribute.
- File extension must not be in its blacklist.
- Directory must not be in its blacklist.
- Filename must not have certain strings from its blacklist.

If **-skipfiles yes/y | no/n** parameter is supplied**, StealBit** will not exfiltrate files with specific filename extensions based on its blacklist.

If **-skipfolders yes/y | no/n** parameter is supplied**, StealBit** will not exfiltrate the contents of the files on the given target directory based on its blacklist.

It avoids a target if the following criteria are met:

- File attribute is **SYSTEM**
- File name has one of the following extensions:

.386	.ocx	.rdp	.part	.exe	.reg	.css	.app	.lockbit
.cmd	.mpa	.bin	.msc	.dll	.mp3	.dmp	.ipa	.theme
.ani	.cpl	.hlp	.spl	.lnk	.mp4	.tmp	.xex	.diagcab
.adv	.mod	.shs	.ps1	.ico	.apk	.pif	.wad	.diagcfg
.msi	.hta	.drv	.msu	.sys	.ttf	.wav	.msu	.diagpkg
.msp	.prf	.wpx	.ics	.cur	.otf	.wma	.icns	.msstyles
.com	.rtp	.bat	.key	.idx	.fon	.dmg	.icns	.gadget
.nls	.ocx	.rom	.woff	.ini	.fnt	.iso	.lock	.sfcache

Table 2 – StealBit File Extension Exclusions

- File name contains one of the following strings:

ntldr	iconcache.db
ntuser.dat.log	thumbs.db
autorun.inf	autorun.inf
bootsect.bak	restore-my-files.txt

Table 3 – StealBit File Name Exclusions

- Folders has one of the following names:

$windows.~bt	google	all users
intel	application data	mozilla
msocache	windows	microsoft.net
$recycle.bin	windows.old	microsoft shared
$windows.~ws	appdata	internet explorer
boot	windows nt	common files
system volume information	msbuild	opera
perflogs	microsoft	windows journal

Table 4 – StealBit Folder Exclusions

ExMatter opts for a more conservative approach, explicitly identifying specific files to collect. It will steal files that meet the following criteria:

- Size of the file must not be less than 1,024 bytes.
- File must not have SYSTEM, DIRECTORY, and TEMPORARY attributes.
- Directory must not be in its blacklist.
- Filename must not have certain strings from its blacklist.
- File extension must be in its target list.

.3ds	.sqlite	.msg	.ts
.accdb	.aspx	.pdf	.xls
.catdrawing	.config	.ppt	.xlsm
.catpart	.cs	.pptx	.xlsx
.catproduct	.csv	.pst	.zip
.dwt	.doc	.sda	
.dxf	.docx	.sdm	
.rdp	.json	.sdw	

Table 5 – ExMatter Target File Extensions

- ExMatter avoids the following:
  - Files smaller than 1024 bytes.
  - File with attribute of:
    - SYSTEM
    - TEMPORARY
    - DIRECTORY

  - Files whose mask and path contains:
    - OneDriveMedTile
    - locale-
    - SmallLogo
    - VisualElements
    - adobe_sign
    - Adobe Sign
    - core_icons
    - C:\Documents and Settings
    - C:\PerfLogs
    - C:\Program Files\Windows Defender Advanced Threat Protection
    - C:\Program Files\WindowsApps
    - C:\ProgramData\Application Data
    - C:\ProgramData\Desktop
    - C:\ProgramData\Documents
    - C:\ProgramData\Microsoft
    - C:\ProgramData\Packages

- C:\ProgramData\Start Menu • \ProgramData\Templates
- C:\ProgramData\WindowsHolographievices
- C:\Recovery
- C:\System Volume Information
- C:\Users\All Users
- C:\Users\Default
- C:\Users\Public\Documents
- C:\Windows
- System Volume Information

ExMatter also builds a queue of traversed target files that will be exfiltrated. It uses the infected system's domain name and hostname for the directory name.

Staging directory: <Domain Name>.<Host Name>

If the domain is not available, it uses the string WORKGROUP:

Staging directory: WORKGROUP.<Host Name>

5.0 Exfiltration

In the versions that Accenture Security analyzed, the network details on where the stolen data will be exfiltrated are hard coded for both exfiltration tools.

StealBit has been promoted as one of the fastest exfiltration tools available. In newer versions of StealBit, the file transfer rate can be configured through the -net/-n or -once/-o parameter. This would allow its affiliates to customize the rate of exfiltration based on the network capacity of its target to avoid suspicion. It also uses HTTP PUT requests, which store and send the file contents as a resource. The data to be sent includes:

- Distributed Authoring and Versioning 2 (DAV2) header.
- Unique identifier decrypted from the config.
- Hostname and domain name (if any) of the compromised system.
- Absolute path of the file being exfiltrated.
- File content that will be exfiltrated.

On the other hand, **ExMatter** provides multiple ways to exfiltrate its stolen data. It primarily uses a **remote SFTP** server to exfiltrate the stolen files. The credentials (username and password) are also hardcoded and is included in the configuration of the malware. If exfiltration through **SFTP** fails more than three times, it will attempt to use a **SOCKS5** proxy as an alternative. Some newer versions added a **WebDAV** client as another alternative.

Countermeasures and Detection Opportunities

The development and utilization of these custom exfiltration tools gives us a glimpse into how these Ransomware groups are adapting over time and creating or updating tools that are better suited for their operations.

It is critical to detect the presence of ransomware operators as early as possible in the attack lifecycle. To protect against the use of exfiltration tools, Accenture Security suggests the following prevention and detection measures:

MITRE Tactic	Eliminate-Control-Observe-Hunt
Execution	*Eliminate:* Employ application whitelisting/blacklisting for specific programs that are not approved for use, including unsigned binaries. *Control*: Wherever possible, limit the execution of PowerShell via use of group policy and endpoint detection and response (EDR) tooling. *Observe*: Monitor PowerShell execution where sender2.exe is the child process or for the deletion of the sender2.exe binary. *Hunt*: Examine PowerShell execution and script block logging for unusual patterns of execution.
Defense Evasion	*Eliminate:* Ensure security tooling has adequate tamper protection as this can be a common pre-deployment tactic utilized by ransomware operators. *Control*: Employ proper system and account hardening to reduce vulnerable or exploitable systems. *Observe*: Monitor for disablement of security tools to include: EDR and anti-virus (AV) as this can be a common pre-deployment tactic utilized by ransomware operators. Hunt: Hunt for execution of unsigned binaries, especially by privileged and administrative accounts.
Discovery	*Eliminate*: Remove data that is past its retention cycle within corporate data governance policies. *Control*: Employ proper network and active directory segmentation to prevent or delay attacker discovery. Observe: Monitoring of tools and APIs used for network process user discovery (Adfind, netscan, NLTest). Hunt: Hunt for file transfer and share-mounting utilities on endpoints.
Collection	*Eliminate*: Wherever possible limit the execution of collection tools, such as 7-zip using group police object (GPO) or EDR.

	Control: Implement robust data loss prevention (DLP) controls with TLS/SSL visibility to restrict outbound network transfers. *Observe*: Monitor for spikes in traffic using common exfiltration protocols and uncommon data flows. *Hunt*: Hunt for evidence of archiving/collection tools present on endpoints, such as 7zip, WinRAR, including command line versions of these tools.
Exfiltration	*Eliminate*: Restrict outbound transfer limits, lock down access to file shares, and implement granular egress policies. *Control*: Block traffic to known C2 infrastructure, non-approved proxy services and anonymity networks. *Observe*: Monitor for traffic to suspicious content delivery networks (CDNs). Monitor for unexpected outbound SFTP traffic to TCP port 22 and WebDAV traffic to TCP port 443. *Hunt*: Hunt for outbound network connections looking for: • Volumetric anomalies by source and destination • Connections to unusual ASNs • WebDAV and SFTP traffic

Table 6 – Countermeasures

MITRE ATT&CK – Tactics & Techniques Observed

TACTIC	StealBit Technique	ExMatter Technique
Execution	T1106: Native API T1559: Inter-Process Communication	T1059.001: PowerShell
Defense Evasion	T1564.003: Hide Artifacts: Hidden Window	T1564.003: Hide Artifacts: Hidden Window
	T1070.004: Indicator Removal on Host: File Deletion	T1070.004: Indicator Removal on Host: File Deletion
	T1027: Obfuscated Files or Information	T1027: Obfuscated Files or Information
Discovery	T1083: File and Directory Discovery T1082: System Information Discovery	T1083: File and Directory Discovery T1082: System Information Discovery
	T1614.001: System Location Discovery: System Language Discovery	
Collection	T1005: Data from Local System	
Exfiltration	T1030: Data Transfer Size Limits T1041: Exfiltration Over C2 Channel	T1048: Exfiltration Over Alternative Protocol

Table 7 – MITRE ATT&CK

Samples Analyzed

File Name	Creation Time	Hash (SHA-256)
sender2.exe	2021-10-15 21:50:53 UTC	b6bc126526e27c98a94aab16989864161db1b3a75f18bd5c72bacbdfccad7bd7
sender2.exe	2021-09-07 04:13:37 UTC	325ecd90ce19dd8d184ffe7dfb01b0dd02a77e9eabcb587f3738bcfbd3f832a1
sender2.exe	2021-10-06 03:05:09 UTC	8eded48c166f50be5ac33be4b010b09f911ffc155a3ab76821e4febd369d17ef
sender2.exe	2021-11-04 23:44:41 UTC	9d056a2fb6ba93e500cdf80d81259cf6386351ce5ef6bf11f4e113f84df8f58f
sender2.exe	2021-11-13 07:30:20 UTC	1018ad95358bcc0c51ec58f5673a285d049bb5e82a5cf83b574ae74472b48dc7
sender2.exe	2021-12-02 23:00:02 UTC	b9f94e4184d6937ea77aead99baaeed8605d58f85a641c1f653896f117a9c2f1
sender2.exe	2021-12-21 22:03:51 UTC	17967fe25627aaf95065f995c70fea1ecee90d5c7ccc775e3ffdf9f08a19450e
sender2.exe	2021-12-10 13:56:26 UTC	080264730f49733e8964437e8a58f1cffc44f7ad3d406dc7fea544a297cf35e3
sender2.exe	2021-12-16 22:08:14 UTC	2d147bce7454dd7898476ee7a15cf22ecaaddd4bc3046a7758dd6562347ff5bd
sender2.exe	2022-01-29 00:27:05 UTC	6d14ea72c28137ed70f58c0f6d6df9c96452e0ba2398a7e8c64ee0fad51b6925

Table 8 – ExMatter-related Hashes

File Name	Creation Time	Hash
StealBit.exe	2021-07-12 04:58:17 UTC	4db7eeed852946803c16373a085c1bb5f79b60d2122d6fc9a2703714cdd9dac0
StealBit.exe	2021-07-31 07:09:59 UTC	2f18e61e3d9189f6ff5cc95252396bebaefe0d76596cc51cf0ade6a5156c6f66
StealBit.exe	2021-07-31 07:09:59 UTC	3407f26b3d69f1dfce76782fee1256274cf92f744c65aa1ff2d3eaaaf61b0b1d
StealBit.exe	2021-07-31 07:09:59 UTC	107d9fce05ff8296d0417a5a830d180cd46aa120ced8360df3ebfd15cb550636
StealBit.exe	-	f1f67fb89c0d1d3a36b086716f276100bc83a3bba2d7318dd3598ff5e2b0d9af
StealBit.exe	-	6c9a92955402c76ab380aa6927ad96515982a47c05d54f21d67603814d29e4a5
StealBit.exe	-	6b9aa479a5f9c6bfee52046c1afa579977dfcde868fdad3f18fdcd1779535068

Table 9 – StealBit-related Hashes

If you have an incident or need additional information on ways to prevent, detect, respond to, or recover from, cyberthreats, contact a member of our CIFR team 24/7/365 by phone 888-RISK-411 or email CIFR.hotline@accenture.com.

About Accenture

Accenture is a global professional services company with leading capabilities in digital, cloud and security. Combining unmatched experience and specialized skills across more than 40 industries, we offer Strategy and Consulting, Interactive, Technology and Operations services — all powered by the world's largest network of Advanced Technology and Intelligent Operations centers. Our 699,000 people deliver on the promise of technology and human ingenuity every day, serving clients in more than 120 countries. We embrace the power of change to create value and shared success for our clients, people, shareholders, partners and communities. Visit us at accenture.com.

Accenture Security is a leading provider of end-to-end cybersecurity services, including advanced cyber defense, applied cybersecurity solutions and managed security operations. We bring security innovation, coupled with global scale and a worldwide delivery capability through our network of Advanced Technology and Intelligent Operations centers. Helped by our team of highly skilled professionals, we enable clients to innovate safely, build cyber resilience and grow with confidence. Follow us @AccentureSecure on Twitter, LinkedIn or visit us at accenture.com/security.