Incidentrapport

Kund Timrå Kommun		Ärendenummer IM447084	
Driftsenhet Malmö		Enhet Quality, Compliance & Information Security	
Upprättad av Krister Svärd	Version P0.2	Dokument datum 2017-06-19	Ansvarig Krister svärd

Beskrivning av incident

2017-05-12 (15:30 CEST) EVRY IRT blev medvetna om kampanjen och har följt utvecklingen sedan dess.
2017-05-12 (15:22 CEST) kom första felanmälan från Timrå Kommun att ett större antal klient PC hade drabbats av denna attack.
Incident Reponse team (IRT) från EVRY etableras för att bistå Timrå Kommuns IT-avdelning.
Beslut tas att Timrå Kommuns IT säkerställer att drabbade PC kopplas fysiskt ur nätverket.
Drabbade användare inaktiveras för att omöjliggöra inloggning.
EVRY säkerställer att samtliga servrar patchas med KB4012213.
2017-05-12 (21:30 CEST) är samtliga servrar patchade
2017-05-15 (11:00 CEST) infekterade klienter ominstalleras på plats
2017-05-16 (15:54) ärendet stängt

Systempåverkan/Tillgängllighet:

Inga data på servrar har påverkats. Filer på drabbade klienter har krypterats och klienterna ominstalleras från standardimage som patchas per automatik med KB4012213.

Systempåverkan/Integritet:

Inga data på servrar har påverkats.

Systempåverkan/Konfidentialitet:

Just nu finns inga indikationer på att information har lämnat nätverket.

Åtgärd:

För att begränsa spridningen patchas samtliga klienter/servers med patch från Microsoft MS (MS17-010)
Återställning av klient PC sker genom ominstallation.

Grundorsak:

För tillfället (2017-05-15) så bedöms det att spridning sker internt nätverk (via SMB1, dvs fildelning mellan enheter). Denna spridning är möjlig genom en sårbarhet som finns i Microsoft Windows. Uppfattningen är att det INTE har spridits primärt via E-mail utan börjat spridas först när en klient blivit infekterad. Viss osäkerhet råder hur en klient blir infekterad. Hos andra användare, utanför Timrå Kommun, har det noterats attackförsök via företagsdatorer som har varit anslutna på hemmanät med bristande säkerhetsnivå, tex med SMB öppet mot Internet. Detta skulle kunna vara ett tänkbart scenario även för användare inom Timrå Kommun.
Att spridningen initialt gick så snabbt bland Timrå Kommuns klient PC berodde på att ett antal klienter inte hade mottagit säkerhetspatch MS17-010 beroende på ett handhavandefel ifrån EVRYs sida vid distributionen av uppdateringar.

Se även bifogad EVRY IRT Note #002 för mer teknisk beskrivning

Långsiktig åtgärd/förslag till förbättring:

Uppgradering av alla klienter till Windows 10. (bättre inbyggt skydd för malware)

Avveckling av befintlig Windows Server 2003 (end-of-life). Ingen garanti för att denna maskin är skyddad.

Införande av övergripande compliance verktyg som åskådliggör och varnar för avvikelser på patchnivå.

Övriga analyser

Genom EVRYs försorg har det gjorts en djupare analys av en specifik användare hos Timrå Kommun som uppfattas som den första drabbade användaren.

Granskning görs av samtliga inkommande mail från Internet (7 st). Inget av dessa mail innehåller något som indikerar att det skulle finnas skadlig kod.

Kontroll görs även av mail som distribuerats internt via Exchange. Inte heller här finns det något som indikerar att spridning skulle ha skett via email.

Skärmdumpar finns som referens vid behov.

Distribution för kännedom:

VD □	Incident Mgr □	SM □	

EVRY IRT Note #002
The WannaCry 2.0 Ransomware Campaign

Released	2017-05-13 01:00, updated 2017-05-13 12:00
Distribution	EVRY Internal + Customers
Author(s)	EVRY IRT/OS
TLP	AMBER: Limited disclosure, restricted to participants organizations

Title	The WanaCrypt0r 2.0 Ransomware Campaign
Criticality	Critical
CVE(s)	MS17-010: CVE-2017-{0143,0144,0145,0146,0147,0148}
Initial disclosure	Approx 2017-05-12 14:00 CET
Known active exploitation?	Yes
Affected systems	Windows client: Vista SP2, 7, 8.1, RT 8.1, ~~10~~[1] Windows server: 2008 R2 SP1 & SP2, 2012 R2 and 2016

Summary

- WanaCrypt0r 2.0 is a major ransomware campaign hitting globally, starting early 2017-05-13 and hitting at least close to 117.000 clients
- The initial infection vector is yet to be determined,
- Upon infection, the malware encrypts files locally and on attached network shares, and a ransom of bitcoins equivalent to initially USD $600 is demanded
- In addition, it leverages the MS17-010 vulnerability in Windows SMB Server to spread laterally within the internal networks of organizations
- Mitigating controls are the usual for combating ransomware: ensuring current and working backups, rapid deployment of security patches as well as user awareness to malicious content distributed via email (described in more detail later in this document)
- At the time of writing, at least three Norwegian organizations were affected, and numerous organizations in Sweden[3]
- Rapid sinkholing by MalwareTech of a ”killswitch domain” that the malware tries to access has most likely sharply reduced the global impact, as the malware exits if it can connect to.

EVRY IRT became aware of the campaign around 2017-05-15:30 CET, and have been tracking it since. At this time, we have no known infections, but we have seen some detections of MS17-010 activity on very few endpoints. Some of these have been verified as triggered by authorized vulnerability scanning, while others are being checked out.

Most of the major antivirus vendors have support[15] against the current set of executables associated with the attack. This combined with early sinkholing of a domain used in the infection process means that the risk is slightly lowered after the initial rush of infections globally. However – we must expect that the attacker will shift attack techniques rapidly – and as long as MS17-010 is unpatched on nodes, the wormlike behaviour of this campaign will remain a significant risk.

[1] According to Microsoft, the attack on Friday did not target Windows 10 nodes: https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/

Description

Around lunchtime CET, the first report that a significant number of computers at Spanish telecom Telefonica was infected[5]. This rapidly expanded to other Spanish companies, followed by a number of UK hospitals, the Russian Interior Ministry, FedEx, Deutsche Bahn[12] and many more.

At the time of writing, companies in various sectors have been affected, so this does not seem to be a campaign targeted at a specific country, sector or company. MalwareInt[2] has a map showing global infections – this map is based on data from sinkholing the C&C node(s) (redirect of network traffic to a destination).

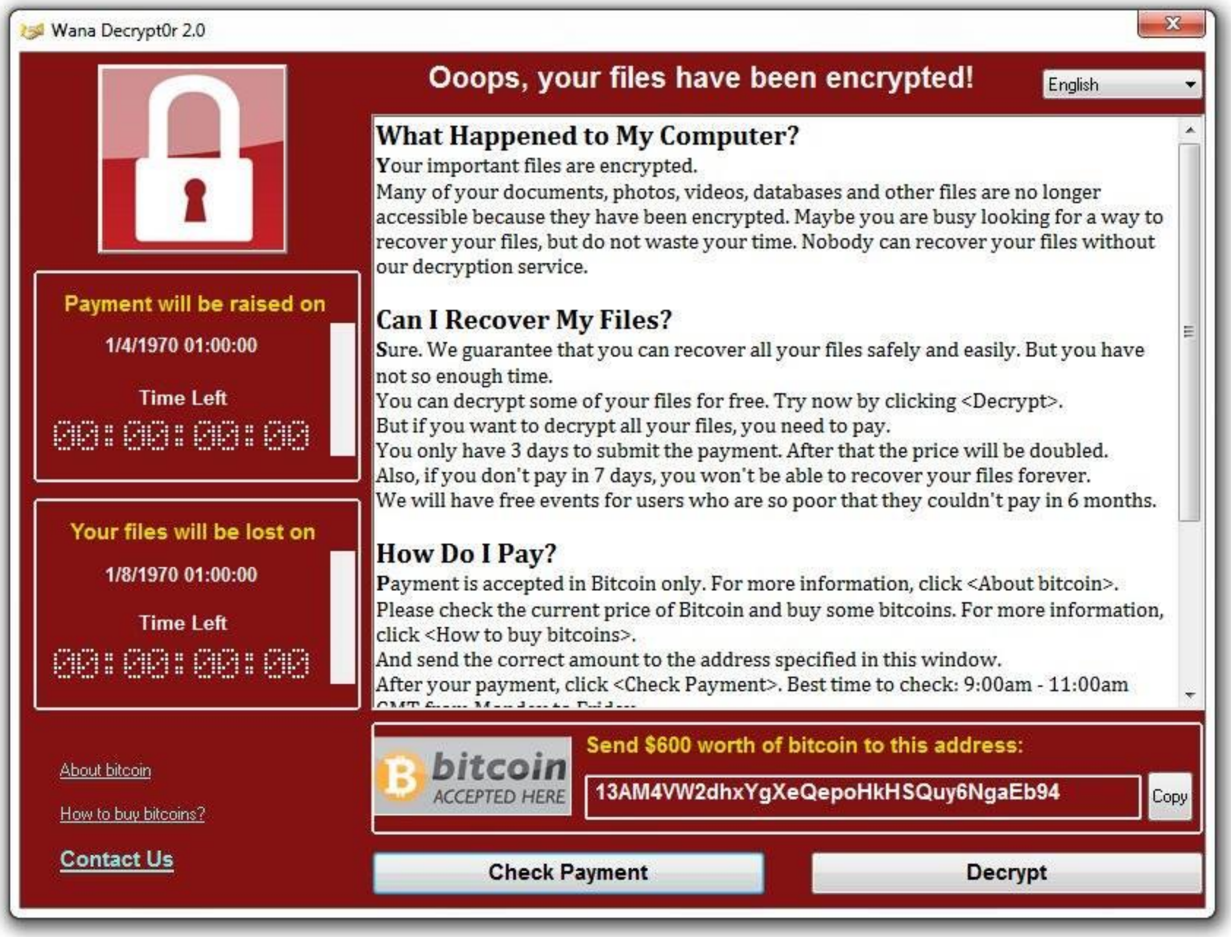
For a good technical overview of the campaign, please see the writeups from Cisco Talos[1], BleepingComputer[10] and Kaspersky SecureList[14], but the condensed version is as follows:

1. The campaign uses two known attack vectors – phishing via mail as well as Internet-based scanning of exposed SMB-talking servers.
2. Once the initial dropper (mssecsvc.exe) runs on a client, it will:
    a. The current executable tries to connect to www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com; if the connetions succeeds, the binary exits.
        i. This domain has now been sinkholed to http1.sinkhole.tech as of 2017-05-12 15:00. Therefore, nothing will happen to any new systems running the executable. The domain was registered on 2017-05-12. It is essential to not block access to this domain, as this will make the malware proceed to encrypt files.
        ii. It will then scan for nodes over 445/tcp for MS17-010 using SMB v1 on the local network, and infect vulnerable nodes. While prevalent earlier, few worm-style attacks has been seen in the past decade. This explains the rapid uptake of infected nodes, as compared to for example the Jaff campaign earlier this week.
        iii. It will also create a second thread 128 times, and scans random hosts on the Internet itself, similar to Conficker and earlier worms. As few organizations expose SMB over the Internet, this is expected to be less successful.
        iv. Successfully compromised nodes will also have the DOUBLEPULSAR implant installed (can be detected using [7])
3. If 2) passes, it installs a service called mssecsvc2.0 ("Microsoft Security Center (2.0) Service"), starts the service, drops the ransomware binary (tasksche.exe) and executes it.
    a. This process then searches local files with a given set of extensions are then encrypted using 2048-bit RSA, and added an extra extension of .WNCRY or .WCRY. It may also scan attached network shares and/or removable devices, but this has not been confirmed.
    b. Concurrently, a Tor client is installed and tries to connect to Tor nodes – enabling the attacker to hide their traffic by routing through Tor.
    c. All files are given full permissions using icacls in order to ensure that a maximum number of files are encrypted.
    d. Shadow copies of files are deleted in order to make recovery more difficuly (done using wmic.exe, vssadmin.exe and cmd.exe) as well as disabling Windows startup recovery and clearing Windows Server Backup history[2].
4. Infected nodes will then show the screenshot reproduced below

[2] `C:\Windows\SysWOW64\cmd.exe /c vssadmin delete shadow /all /quiet & wmic shadowcopy delete & bcdedit /set {default} boostatuspolicy ignoreallfailures & bcdedit /set {default} recoveryenabled no & wbadmin delete catalog -quiet`

    a. The malware contains translations for a large number of languages, so the text may differ.
5. At the time of writing, one of the bitcoin accounts tied to the attack is around NOK 1.5 million., indicating that a significant number of organizations/people have been paying the ransom

It must be expected that the attackers will release modified executables in the near future and/or shift their attack delivery mechanisms. One sample tied to this outbreak is linked to as [11] and [13].



Ooops, your files have been encrypted!

Payment will be raised on 1/4/1970 01:00:00

Your files will be lost on 1/8/1970 01:00:00

What Happened to My Computer?
Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?
Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am GMT from Monday to Friday.

Send $600 worth of bitcoin to this address:
13AM4VW2dhxYgXeQepoHkHSQuy6NgaEb94

Mitigating Actions

- Ensure that backups are current, complete and working
- Ensure that all systems are patched for MS17-010
    - Windows Server 2003 cannot be patched for this, so potentially remaining nodes will be at risk for infected clients
- Block Tor exit nodes[9] at the firewall level
- Implement write blocking of selected[6]
- Ensure that SMB traffic is blocked on all externally exposed nodes (port 139 and 445) as well as RDP
- Disable the SMB v1 protocol[17] (or limit it to strictly segregated zones)
- Disassociate .hta and .js files from Windows Script Host (and possibly map them to Notepad.exe) (possibly others as well)
- Consider blocking incoming attachments on mail gateways
- Ensure that antimalware signatures are up-to-date
- Employing AppLocker[8] to control which applications an user may run

- Eradicate out of support systems like Windows Server 2003 if necessary, install out-of-band patches from Microsoft
- Not allowing general end users to have Local Admin
- Web proxy filtering of utilized files (.hta files are believed to be used in this attack)
- General user security awareness when it comes to suspicious emails (attachments and links)

Known Indicators of Compromise

Please see [1] and [10].

References

1. http://blog.talosintelligence.com/2017/05/wannacry.html
2. https://intel.malwaretech.com/botnet/wcrypt
3. https://www.cert.se/2017/05/pagaende-ransomware-kampanj-wannacry-wcry-wannacrypt0r
4. https://blog.malwarebytes.com/threat-analysis/2017/05/the-worm-that-spreads-wanacrypt0r/
5. http://elpais.com/elpais/2017/05/12/inenglish/1494588595_636306.html
6. https://github.com/nexxai/CryptoBlocker
7. https://github.com/countercept/doublepulsar-detection-script
8. https://technet.microsoft.com/en-us/library/ee424367(v=ws.11).aspx
9. https://check.torproject.org/exit-addresses
10. https://www.bleepingcomputer.com/news/security/wana-decryptor-wanacrypt0r-technical-nose-dive/
11. https://www.virustotal.com/en/file/09a46b3e1be080745a6d8d88d6b5bd351b1c7586ae0dc94d0c238ee36421cafa/analysis/
12. https://twitter.com/uwepleban/status/863121674090283009
13. https://www.hybrid-analysis.com/sample/24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c?environmentId=100
14. https://securelist.com/blog/incidents/78351/wannacry-ransomware-used-in-widespread-attacks-all-over-the-world/
15. https://www.virustotal.com/en/file/24d004a104d4d54034dbcffc2a4b19a11f39008a575aa614ea04703480b1022c/analysis/
16. https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/
17. https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/
18. https://securingtomorrow.mcafee.com/executive-perspectives/analysis-wannacry-ransomware-outbreak/
19. https://www.troyhunt.com/everything-you-need-to-know-about-the-wannacrypt-ransomware/
20. Steven M. Bellovin: Patching is Hard: https://www.cs.columbia.edu/~smb/blog/2017-05/2017-05-12.html
21.