BITPAYMER/IENCRYPT RANSOMWARE

21/10/2019

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

Table of contents

BitPaymer, also known as FriedEx or IEncrypt, is used since at least July 2017. It is used against private and public entities in targeted attacks, manually operated [1].

Research from security company ESET [2] linked BitPaymer to Dridex[1] (sophisticated banking Trojan used since 2014 and known to target financial sector) sharing multiple technical similarities with the latter. Threat Actor operating Dridex could have diversified its lucrative activities, learning from success stories of earlier ransomware.

1 Infection methods and salient facts

Sometimes, BitPaymer is distributed through compromised legitimate websites delivering malevolent Flash and Chrome updates[3]. It has also been observed to be delivered through weakly protected RDP accesses [1]. In July 2019, BitPaymer's victims were compromised via phishing campaigns [4]. Theses multiple methods of infection could point out that BitPaymer is sold on black markets as a RaaS (Ransomware-as-a-Service) and used by different Threat Actors, designated as "Affiliates".

In the majority of the BitPaymer's attacks ANSSI has known of, Threat Actors propagated manually **for approximatly one week** within the victim's network before the ransomware deployment. To perform the propagation, Threat Actors firstly sought to compromise network administrators accounts in order to take control of central servers, such as Active Directory. Theses accounts serve also to indentify critical ressources within the network (File system storage, data backup, production-related equipments). Use of Dridex banking trojan, Pentest tool Powershell Empire, credentials viewer tool Mimikatz and administration tool PsExec have been reported. After taking over the network's administrators accounts, Threat Actors use them to deploy the ransomware over the week-end and night, firstly on DC servers, critical ressources, **including on data backup systems**, to maximise impact.

In addition to the encryption of accessible files, BitPaymer is able to deactivate some AV products and to wipe shadow copies of file systems.

It is worth noting that BitPaymer is packed with a custom code, compiled only a few hours before the attack. With this technique, Threat Actor can use BitPaymer code without modifying it to evade detection [4].

Finally, ransom notes issued by BitPaymer are identifiable by the systematic mention of the victim company name and the combination of two contact email addresses: one in tutanota.com, the other in protonmail.com with evidently generated pseudonym.

1.1 TTP MITRE ATTACK

Kill chain step	TTP	Comments
Initial Access	Spearphishing Attachment	Attachment or link
Initial Access	Spearphishing link	Attachment or link
Initial Access	Trusted Relationship	Subcontractors or ESN compromises
Execution	Command-Line Interface	arp / nslookup / etc.
Execution	Service Execution	Alternate Data Stream
Persistence	Hidden Files and Directories	Alternate Data Stream
Persistence	Modify Existing Service	
Privilege Escalation	Bypass User Account Control	
Privilege Escalation	Exploitation for Privilege Escalation	Apple Update 0-day
Defense evasion	Bypass User Account Control	
Defense evasion	Deobfuscate/Decode Files or Information	
Defense evasion	Disabling Security Tools	Windows Defender
Defense evasion	Exploitation for Defense Evasion	Windows Defender
Defense evasion	Obfuscated Files or Information	Encrypted strings with RC4
Defense evasion	Software Packing	Custom Packer Code

[1] A malware used to exfiltrate banking-related credentials that can also download other malwares

Discovery	Account Discovery	
Discovery	System Network Connections Discovery	
Command and Control	Data Obfuscation	Empire
Command and Control	Multilayer Encryption	Empire
Command and Control	Standard Cryptographic Protocol	Empire
Impact	Data Encrypted for Impact	
Impact	Disk Content Wipe	
Impact	Inhibit System Recovery	

2 Victimology

On the 25th of August 2017, Bitpaymer notably compromised multiples Scottish hospitals [5]. Entities in education, manufacturing, finance and agriculture industries were also targeted [4].

3 DoppelPaymer variant

In July 2019, a new variant of the BitPaymer ransomware was detected by Crowdstrike [6] (dubbed as DoppelPaymer), showing significant differences with the original ransomware. DoppelPaymer ransomware was used against the US municipality of Edcouch, Texas. BitPaymer incidents continuing at the same period of time, Crowdstrike believes this new variant to be a sign of a split within the Threat Actor team responsible of the development of BitPaymer.

This new variant gives some clues about cybercriminal habits, particularly their will to adapt their attacks as much as possible to the financial capacity of their targets. Consequently, Doppelpaymer attacks were associated with largely variable ransom amounts, from 2 to 100 Bitcoins.

4 Recommandations

Upon loading, BitPaymer checks if the file ”`C:\\aaa_TouchMeNot_.txt`” [4]. exists. If so, BitPaymer will terminate the execution, so that it'll not execute itself in the Windows Defender Emulator. By creating this file, it's possible for defenders to thwart the infection.

To prevent as much as possible the payload execution, a machine's hardening must be done (file execution control, behavioral analysis). ”Backup-less” architecture which aimed to protect effectively against isolated data destruction, do not protect against ransomware attacks, beause attack groups target replicated data servers. Thus, disconnected backups for critical data are highly recommended.

Finally, Active Directory once ciphered can critically affect the information system integrity. A multi tier approach, with recommended security administration has to be implemented to make sure privileged accounts are not accessible by attack groups (see Microsoft "Active Directory administrative tier model").

5 Detection

In July 2019, the security company Morphisec published a excellent Yara rule to detect the BitPaymer's Custom Packer code [4]. ANSSI confirms this rule allows to detect the obfuscation layer of BitPaymer.

```
rule BitPaymer {
        meta:
                description = "Rule to detect newer Bitpaymer samples. Rule is based on BitPaymer custom packer"
                author = "Morphisec labs"
        strings:
                $opcodes1 = {B9 ?? 00 00 00 FF 14 0F B8 FF 00 00 00 C3 89 45 FC}
                $opcodes2 = {61 55 FF 54 B7 01 B0 FF C9 C3 CC 89 45 FC}
        condition:
                (uint16(0) == 0x5a4d) and ($opcodes1 or $opcodes2)
}
```

Source code part 5.1: Yara rule for BitPaymer's Custom Packer code. Source : Morphisec

Furthermore, drastic behaviour modifications of network administrators accounts (for example extensive use of RDP connections) could help detect lateralization phase of a BitPaymer attack.

Finally, performing signature-based detection on Powershell Empire and Dridex banking trojan could help stopping BitPaymer attack before the ransomware deployment. ANSSI has discovered some IP addresses currently associated with PowerShell Empire alive servers.

6 Bibliography

[1] NJCCIC. *Bit Paymer*. Aug. 29, 2017. URL: https://www.cyber.nj.gov/threat-profiles/ransomware-variants/bitpaymer.

[2] ESET. *Dridex Authors Return with a New Chapter in Their Malware Story*. Jan. 26, 2018. URL: https://www.welivesecurity.com/2018/01/26/friedex-bitpaymer-ransomware-work-dridex-authors/.

[3] CrowdStrike. *Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware*. Nov. 14, 2018. URL: https://www.crowdstrike.com/blog/big-game-hunting-the-evolution-of-indrik-spider-from-dridex-wire-fraud-to-bitpaymer-targeted-ransomware/.

[4] Morphisec. *BitPaymer Ransomware Leveraging New Custom Packer Framework Against Targets Across the U.S.* July 19, 2019. URL: http://blog.morphisec.com/bitpaymer-ransomware-with-new-custom-packer-framework.

[5] BleepingComputer. *Bit Paymer Ransomware Hits Scottish Hospitals*. Aug. 29, 2017. URL: https://www.bleepingcomputer.com/news/security/bit-paymer-ransomware-hits-scottish-hospitals/.

[6] Crowdstrike. *CrowdStrike Discovers New DoppelPaymer Ransomware & Dridex Variant*. July 12, 2019. URL: https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/.

- 21/10/2019

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ANSSI - 51 boulevard de la Tour-Maubourg, 75700 PARIS 07 SP
www.cert.ssi.gouv.fr / cert-fr.cossi@ssi.gouv.fr

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Premier ministre

SGDSN