
CYBERARK®
RANSOMWARE EXPOSED
Key Learnings from Examining 3.5 Million Samples

ANDY THOMPSON

Andy.Thompson@CyberArk.com

- Linkedin: in/andythompsoninfosec
- GitHub: github.com/binarywasp
- Twitter: @R41nMkr

- Global Research Advisor
- SSCP/CISSP
- GPEN Pen-tester
- Dallas Hacker
- Travel-Hacker

RANSOMWARE

- Leveraging technical controls to inhibit use of data.
- Operates under the assumption that the data is important enough that users are willing to pay for recovery.
- There is no guarantee of actual recovery, even after payment is made.

WHY RANSOMWARE WORKS

- Fail to practice good hygiene.
- Using ineffective methods.

THE FIRST RANSOMWARE

- Discovered in 1989
- Replaced Autoexec.bat
  - After 90 boots, Encrypted file names on c:/
- Asked to ‘renew the license’
  - $189 to a PO box in Panama
- Dr. Joseph Popp was arrested by Scotland Yard later that year and charged with blackmail

INTERNET ERA RANSOMWARE: REVETON

- **Reveton Trojan Family**
  - Impersonates national law enforcement
  - Locks out of PC
- **Easily removed**
  - Boot to safemode
  - Remove registry key

CRYPTO-CURRENCY

- **Bitcoin**
  - Anonymous
  - Secure
  - Instant
  - Not regulated
  - Perfect for **EXTORTION!**

MAZE

- Ransomware as a Service.
- Work as affiliated network of teams.
- Leak users' files in addition to encrypting.
- Attackers threaten to publish data if ransom is not paid.
- Advanced tactics for lateral movement.
- "Shut down" 11/1/2020.

CORONAVIRUS

- Propagates via coronavirus messaging.
- Deletes backups before encryption of files.
- Low ransom amount (USD$45-60)
- Also drops credential stealer (Kpot/Khaleesi)

```
!!!!!CORONAVIRUS is there!!!!

All your file are crypted.
Your computer is temporarily blocked on several levels.
Applying strong military secret encryption algorithm.

To assist in decrypting your files, you must
Pay to Bitcoin wallet: bc1qkk6nwhsxvtp2akunhkke3tjcy2wv2zkk00xa3jcontact us
 via e-mail: coronavi2022@protonmail.ch
Donations to the US presidential elections are accepted around the clock.
Desine sperare qui hic intras! [wait timeout 15 min]
```

Browser	Messaging & Voice Call	Virtual Coins	Windows	Banking	File Transfer Protocol Clients	VPN	Gaming
Chromium based browsers	Skype	Etherum	Harvest User Credentials	Credit Cards	FileZilla	NordVPN	Steam
Mozilla based browsers	Telegram	Electrum	General Machine Information		Winscp	EarthVPN	Battle.Net
Internet Explorer	Discord	Bytecoin			TotalCommand		
	PSI	Namecoin			IPSwitch		
	Pidgin	Monero					

EKANS

- Not a pokemon.
- Not affiliated with APT.
- Targets ICS/SCADA Systems.

SNATCH

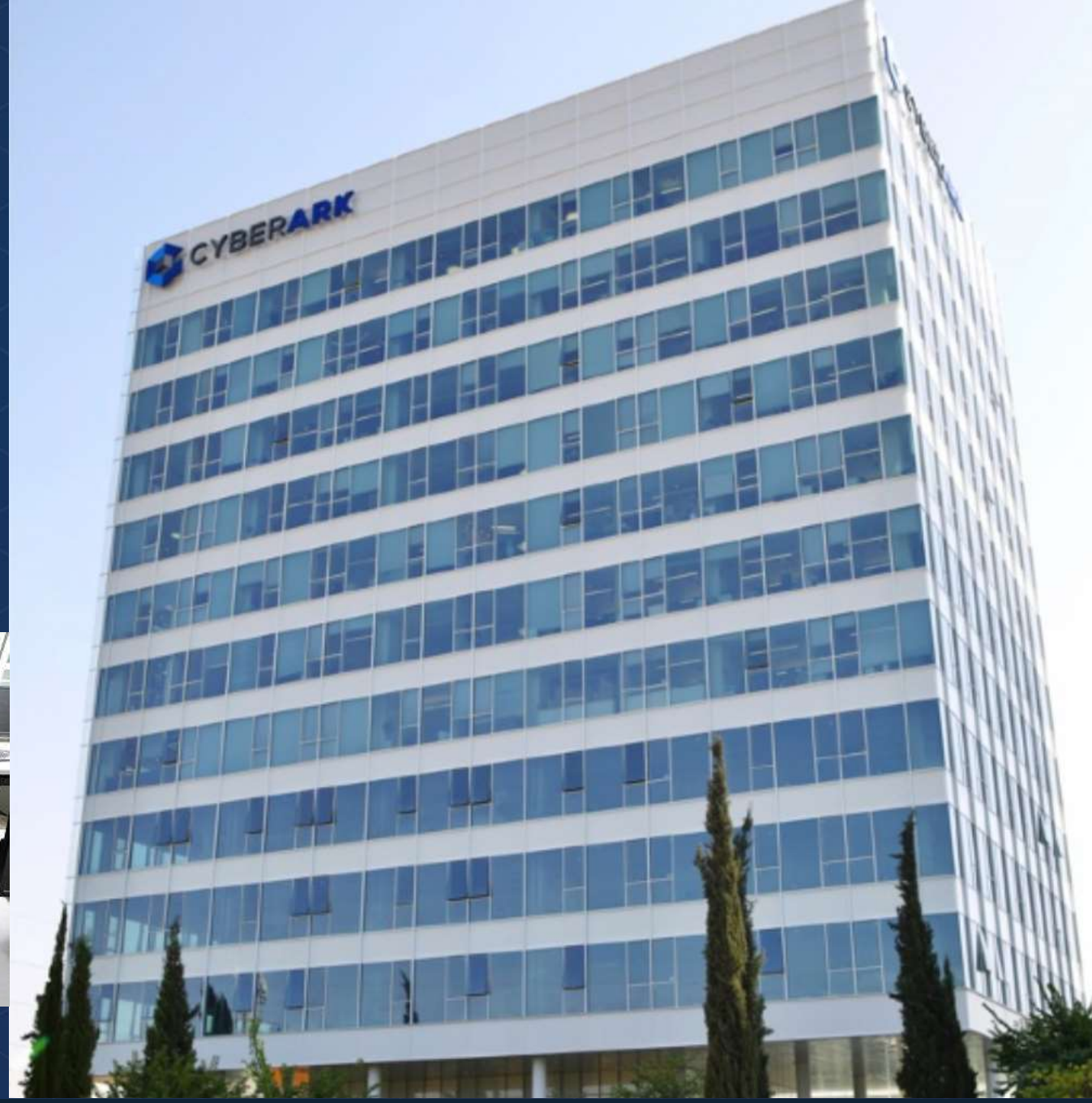
- Creates service & reboots machine.
- Boots into Safe-Mode.
- Bypasses AV & EDR.

DONALD TRUMP

Builds a wall around your files and…
makes you pay for it!

CYBERARK LABS

- In house team.
- Physical lab.
- 3.5 Million + samples.



DOCX ENCRYPTED All Time

0

RANSOMWARE All Time

SHA256	All Time
4b058c6cdfe223c9178bc56e9db00e5b6db92c405fdc8ccb9008b83ea5309cd1	20210422
da68ca8ffbe0d4e3e80c5d87bc7ee6315eb33ae98bf251a04dce71a710d23238	20210415
2641ad190b60cdde7f0c6285d7de2e538bd7b94c461c7be50e59474deff50b1e	20210415
92815be6471287eb405fe74ee85ed000821d4d6f8c9e0154b289be8b2e7c7e5d	20210404

SAMPLES CHECKED All Time

3,494,258

RANSOMWARE FAMILES All Time

THREAT COUNTRIES All Time

Metrics	All Time
CA	1,592,789
US	1,507,826
FR	704,101
KR	226,635
UA	187,661
DE	145,440
AR	123,084
ZZ	120,586

SAMPLE FILES All Time

ACTIVE MACHINES Today (Apr 27)

35

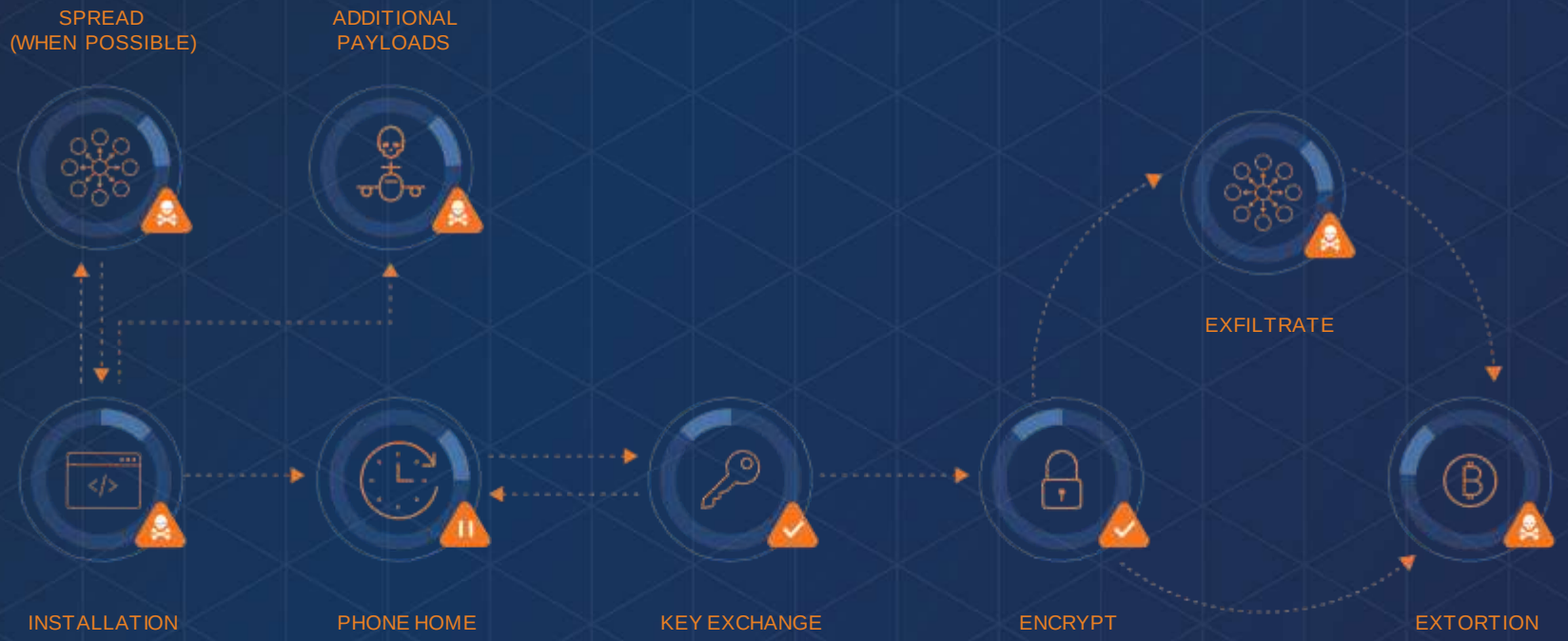
SAMPLES DOWNLOADED/CHECKED Last 7 days (Apr 20 - 26)

1,763

Ransomware Lab

Date Range | last update an hour ago | Powered by databox

RANSOMWARE KILL-CHAIN



RELIANCE ON UNIQUE ENCRYPTION KEY

70%

Asked for a unique key from the key server; proceeded with default key if unavailable.

10%

Required unique key embedded in file

20%

Required unique key from key server; failed if unavailable


CYBERARK
MITIGATION STRATEGIES

BACKUP & RECOVERY

- Allows recovery without payment.
- Part of every Disaster Recovery strategy.
- Does not prevent ransomware attacks.
- Data may still be lost.
- Costs of storage and data loss should be considered.

LEAST PRIVILEGE

- Part of Microsoft's "Ten Immutable Laws of Security".
- Prevents only 10% of ransomware analyzed.
- Potential challenges with productivity.

BLOCK LISTING APPLICATIONS

- Prevents KNOWN malware.
- Ineffective against new & polymorphic ransomware.

ALLOW LISTING APPLICATIONS

- 100% effective against ransomware.
- Difficult to execute effectively.
- Easier implemented on servers.
  - More difficult for user endpoints.

GREYLISTING APPLICATIONS

- Allows more flexibility.
- Restricts:
  - Internet access (Geo-callbacks/key exchange)
  - Read, Write, & Modify file permissions.

- 99.97% Effective **with Local Admin privilege**
- 100% Effective **without Local Admin privilege**

RECOMMENDATIONS

- Use Anti-virus and EDR.
- Backup.
- Restrict applications read/write/modify permissions.
- Allow only approved applications when possible.
- Remove local admin rights from standard users.
- Elevate privileges when needed.
- Assess which file types are most valuable to the organization.

SUMMARY

Alternate approach to proactive security is effective against ransomware.

- Least Privilege
- Application Control
- 💯 Effective