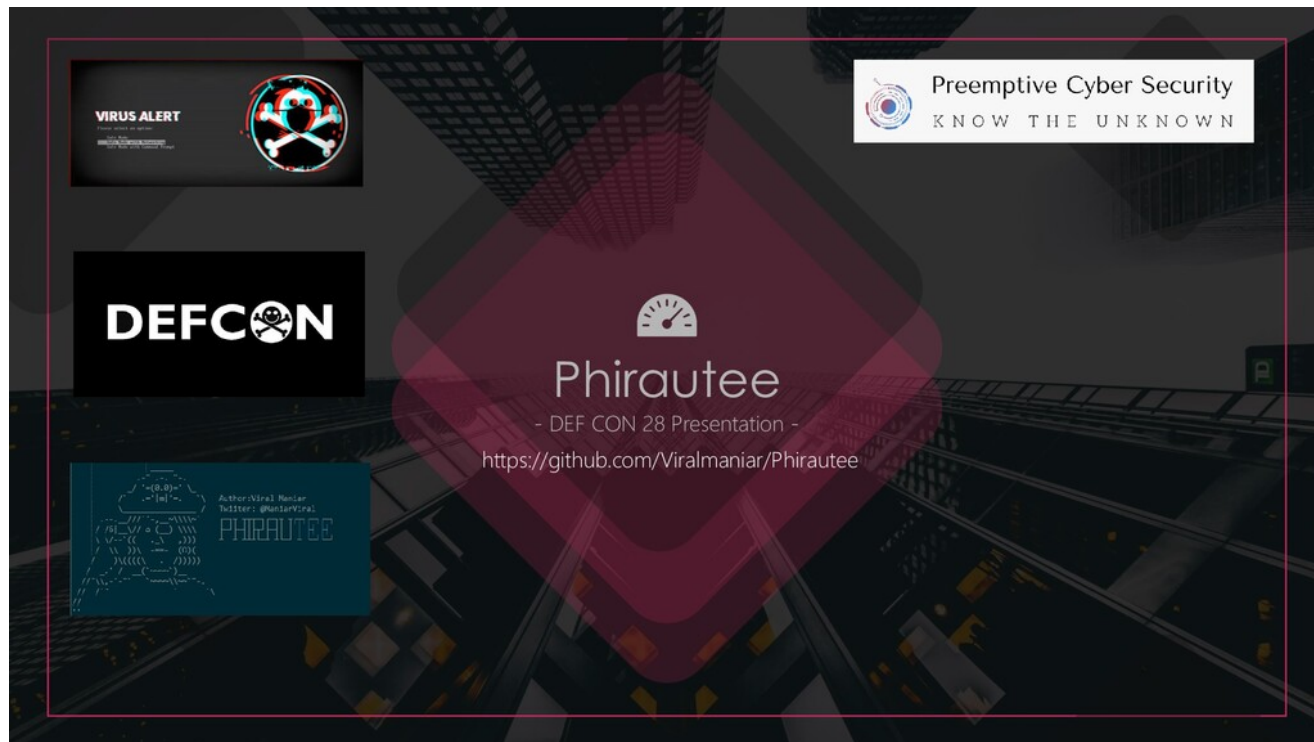


# Phirautee - DEFCON28 - Writing Ransomware using Living off the Land (LotL) Tactics

[speakerdeck.com/viralmaniar/phirautee-defcon28-writing-ransomware-using-living-off-the-land-lotl-tactics](https://speakerdeck.com/viralmaniar/phirautee-defcon28-writing-ransomware-using-living-off-the-land-lotl-tactics)



August 08, 2020

Over the past few years, ransomware has gone wild and organisations around the world are getting targeted leading to the damage and disruption. As we all know that the threat landscape is changing rapidly and we hear the fuss about ransomware infection at the offices or read about it in the news. Have you ever wondered how threat actors are writing

ransomwares? What level of sophistication and understanding is required to target an organisation? In this demo, we will utilise the native Windows commands to build ransomware and target a host via phishing. Introducing Phirautee, a proof of concept crypto virus to spread user awareness about attacks and implications of ransomwares. Phirautee is written purely using PowerShell and does not require any third-party libraries. This tool steals the information, holds an organisation's data to hostage for payments or permanently encrypts/deletes the organisation data. The tool uses public-key cryptography to encrypt the data on the disk. Before encrypting, it exfiltrates the files from the network to the attacker. Once the files are encrypted and exfiltrated, the original files are permanently deleted from the host and then tool demands a ransom. The ransom is asked using the cryptocurrency for payments, so transactions are more difficult for law enforcement to trace. During the demonstration of Phirautee, you will see a complete attack chain i.e. from receiving ransomware attack via a phishing email and how the files get encrypted on the compromised systems. A detailed walkthrough of the source code would be provided to understand how hackers utilise simple methods to create something dangerous. I will end the demo with several defence mechanisms by performing forensics analysis on Phirautee using publicly available tools.

## More Decks by ViralManiar

---


[See All by ViralManiar](#)

## Other Decks in Technology

---

[See All in Technology](#)

[srenext2022-skaru](#)

 [mixi\\_engineers](#)

[PRO](#)

[1](#)

[1.1k](#)

Graph API について



miyakemito

0

330

NestJS + Prisma2 で歩む RLS の世界



ynaka81

1

100

Microsoft Build 2022 - Azure のデータ & 分析サービス 最新アップデート / Microsoft ...



nakazax

1

220

プロダクトの理想と現実はなぜ乖離しがち？プロダクト作りに潜む問題を考える



suzukentaro

0

270

1年間のポストモーテム運用とそこから生まれたツール sre-advisor / SRE NEXT 2022



fujiwara3

6

3.8k

ニフティでSRE推進活動を始めて取り組んできたこと



2

850

長年運用されてきたモノリシックアプリケーションをコンテナ化しようとするどん...



PRO

15

8.1k

數據的多重宇宙 @ LINE Taiwan



PRO

0

1k

Puny to Powerful PostgreSQL Rails Apps



andyatkinson

PRO

0

410

[SRE NEXT 2022]KaaS桶狭間の戦い～Yahoo! JAPANのSLI/SLOを用いた統合監視～



srenext

0

690

プルリク作ったらデプロイされる仕組み on ECS / SRE NEXT 2022



carta\_engineering

1

670

## Featured

---

See All Featured

A Philosophy of Restraint



\_colly.

192

14k

Writing Fast Ruby



sferik

612

57k

Learning to Love Humans: Emotional Interface Design



aaron

261

37k

Designing with Data



zakiwarfel

91



3.9k

WebSockets: Embracing the real-time Web



robhawkes

57

5k

How GitHub Uses GitHub to Build GitHub



holman

465

280k

Build The Right Thing And Hit Your Dates



maggiecrowley

19

1.2k

Fontdeck: Realign not Redesign



paulrobertlloyd

73

4.1k

Producing Creativity



orderedlist

PRO

333

37k

How GitHub (no longer) Works



holman

296

140k

Fantastic passwords and where to find them - at NoRuKo



philnash

25

1.5k

Building Better People: How to give real-time feedback that sticks.



wjessup

343

17k

## Transcript

---

1. **Phirautee - DEF CON 28 Presentation -**  
**<https://github.com/Viralmaniar/Phirautee>**

---

2. **LEGAL DISCLAIMER 2 • 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.

3. **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 <https://github.com/Viralmaniar>  
<https://twitter.com/maniarviral> <https://www.linkedin.com/in/viralmaniar/>  
<https://viralmaniar.github.io/>

#### 4. AGENDA Your Logo Here 4 • 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 Phirantee tool and setup guide • Demo - Phirantee • Mitigation strategies • Final words on some of the community projects

#### 5. STEALING – OLDEST CRIME Your Logo Here 5

---

#### 6. RECENT RANSOMWARE ATTACKS 6

---

#### 7. 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.

#### 8. HOW DO I KNOW IF I AM INFECTED? 8 •

---

Ransomware is usually considered as one of the nosiest 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:

#### 9. WANNACRY HACKED EVERYTHING 9

---

#### 10. 32 58 638 184 204.24 187.9 0 100 200 300

---

400 500 600 700 12/31/2015 12/31/2016 12/31/2017 12/31/2018 12/31/2019  
07/30/2020 Ransom Attacks Remote Services 51% Phishing Emails and Social  
Engineering 38% Software vulns 8% Torrent, Cracked Software or USB attacks 3%  
“Most of the ransomware attacks are opportunistic“ Ransomware attacks: 2015- 2020  
(Q1) ATTACK STATISTICS AND INFECTION METHODS 10

11. **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.

12. **XDEDIC 12 • 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.

[https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07191218/xDedic\\_marketplace\\_ENG.pdf](https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/07191218/xDedic_marketplace_ENG.pdf)

13. **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.

14. **31865 12089 15761 377027 779856 1339878 157445 71063 327931 0**

---

500000 1000000 1500000 Q3 2019 – Q4 2019 - Q1 2020 Sodinokibi Ryuk Phobos 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 Average Ransom Payments: Top 3 Types

15. **TARGETED INDUSTRIES 15 60% 56% 55% 54% 50% 49% 49%**

---

48% 46% 45% Industries victim of ransomware attacks Media & Entertainment IT & Telecom Energy, oil/gas & utilities Other Business & professional services Construction & property Retail, distribution and transport Financial services Manufacturing and production Public Sector E-Sports Entertainment, Travelex , NHS, Honda Toll Group, Deutsche Bahn, Maersk, FedEx Garmin, IN SPORT, Lion, E-Sports Entertainment In the last year, has your organisation been hit by ransomware? Base: 5,000 respondents. (THE STATE OF RANSOMWARE 2020 ) – Sophos white paper Blackbaud, Argentine Telcom, UCSF, Cognizant

## 16. Upcoming Deposits Market Place Over 150 countries got infected ATTACK

---

SUMMARY 16 300,000+ Latest Ransom: \$10 Million \$ 84,116 Organisations sustained attacks: 205, 280 › 1,150% increment in 2019 › Victim paid avg \$20,000 Victims around the world Crypto (70-80%) Other (7%) Infrastructure (10%) Gift Card (13%) Ransom amount gets cashed out using cryptocurrency exchanges. Buy online gift cards Buy new attack infra Drugs, games etc 0 20 40 RDP SSH Persistence with RAT SSH - RDP \$1,500 \$6 - \$350 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.

## 17. INTRODUCING PHIRAUTEE 17 • 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

## 18. PHIRAUTEE ATTACK SETUP 18 • 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: • Throwing away 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>

## 19. USE OF CRYPTOGRAPHY IN PHIRAUTEE 19 • 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. Symmetric Key Cryptography Asymmetric Key Cryptography

## 20. **SYMMETRIC KEYS & ANON SMTP 20 • 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.

## 21. **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?

## 22. **TRY UNTIL YOU CAN BYPASS 22**

---

## 23. **DEMO TIME! 23**

---

## 24. **IOCS FOR PHIRAUTEE 24 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%\PhirauteeBackground-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

## 25. **HOW CRIMINALS CONVERT RANSOM TO CASH? 25** **<https://bitshills.com/best-non-kyc-crypto-exchanges/>**

---

## 26. **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.



27. **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.

28. **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://id-ransomware.malwarehunterteam.com/>  
<https://www.nomoreransom.org/>

29. **WWW.NOMORERANSOM.ORG 29**

---

30. **ID-RANSOMWARE.MALWAREHUNTERTEAM.COM 30**

---

31. **31 Image from: [https://www.metacompliance.com/wp-content/uploads/2020/03/Ransomware\\_Guidelines\\_Point\\_8\\_png\\_BuYG-A-N6.png](https://www.metacompliance.com/wp-content/uploads/2020/03/Ransomware_Guidelines_Point_8_png_BuYG-A-N6.png)**

---

32. **THANK YOU**

---