DEFINING TODAYS ATTACKER

NOUREEN NJOROGE

TIM GURGANUS

CHRIS RILEY

DEFINING TODAYS - NOTES

- Four sections:
  - Profiles of todays hackers – Tim
    - Targeted Ransomware
      - Ryuk, SAMSAM
    - Iran Pentest etc.
    - Carding Groups (Skimmers Magecart etc)
    - Extortion Attacks
      - DDOS – IOT Bots etc.
      - Sextortion
  - Services – Provide a definition and example for each – Combine with Cashout?
    - Malware as a service -
    - Phishing as a service
    - Tool developers
      - Obfuscation services

NOTES CONTINUED

- Cash Out Methods or Fame - Riley
  - How do they make money
  - Cross shipping
    - Stolen credit cards etc.
  - Ransomware payments and amount of money
  - Coin Mining
- Defense IN-Depth Q/A - Noureen
  - Which type of security controls work
  - Network controls
  - Endpoint controls

Profiles – groups and individuals in crime

Account Take Over – Identity Theft
- Phishing
- Credentials – Discord tokens, passwords, Oauth tokens
- Game Accounts
- Bank fraud – Bank acct. info
- Gift card fraud
- Crypto currency fraud
- Health Insurance fraud
- Social Network Stat accounts

Profiles – groups and individuals in crime

State Sponsored (APT)

- Espionage for Economic gain from theft of IP, market research
- Espionage for Political gain by data gathering, geo tracking

Profiles – groups and individuals in crime

Financial Fraud

- Credit Carding Groups (Skimmers Magecart etc)
- Bank acct. infostealers

Profiles – groups and individuals in crime

Extortion Attackers
- DDOS – IOT Bots etc.
- Sextortion
- Targeted Ransomware
  - Ryuk, SAMSAM
- Iran Pentest etc.

Profiles – groups and individuals in crime

Exploit developer – Web Browser, OS Kernel, MS Office, Android, iPhone, Wordpress, Apache, IIS, Oracle, SAP, Linux, Cisco, OSX
Exploit brokers
Malware Author – Infotealer, Ransomware, Coin Miner, RAT, Rootkit, Webshell, Click Fraud, Mobile Malware
Document Exploit Kit developer
Phishing Kit Author

Profiles – Modus Operandi

- Mass delivered malware
- Mass exploit scan
- Mass phishing
- Targeted malware
- Targeted exploit scanners
- Targeted phishing

DEFINING TODAYS - NOTES

- Four sections:
  - Profiles of todays hackers – Tim
    - Targeted Ransomware
      - Ryuk, SAMSAM
    - Iran Pentest etc.
    - Carding Groups (Skimmers Magecart etc)
    - Extortion Attacks
      - DDOS – IOT Bots etc.
      - Sextortion
  - Services – Provide a definition and example for each – Combine with Cashout?
    - Malware as a service -
    - Phishing as a service
    - Tool developers
      - Obfuscation services

Cyber Crime Services

Exploit Kit Services
malSpam distribution services
Bullet Proof hosting
Botnet services – exploit scanners, dictionary attack/credential stuff services for portals (amazon, ebay, paypal, airline miles, giftcards, facebook, gmail, instagram, icloud)
Malvertising services – hacked Ad domains, advertising accounts on social media such as Facebook
Botnet hosting
Fastflux DNS services
Malware packaging – FUD services, Obfuscation services, downloader services, Evasion services, packers, Digital signing, Sandbox evasion, anti-VM, anti-analysis, anti-forensics, polymorphic
Exploit Kit as a Service (Windows browser, malDoc, Android Browser, iPhone browser, iPhone jail break, Android root)
0-day exploits (IE, Firefox, Android, iPhone, Apache, IIS, MS Office, Safari, Java, Flash Player

Cyber Crime Services

Installation as a service
Malware as a service
Ransomware as a service
Social Networks hacking services – Jacking
Tech support scammers
Romance fraud
Phishing as a Service
Web server attack tools – SQL injection, blind SQL injection, RFI, Wordpress
POS malware
ATM malware – jackpotting
Exploit frameworks – Core, Cobalt Strike, PlugX, YTY
Play Store / App Store distribution
Target list services (email, social media account names)

Cyber Crime Services

Search Engine Optimization
Hash cracking services
Domain takeover
Similar domains, Certificate fraud
Spambot
Vishing
Smishing
RoboCalls

Cyber Crime Services

Remote Access services – Server with certain speed/cores/software, RDP, SSH, PSN, Fortnite, Steam, VPN, compromised VPN credentials
Stat accounts - Followers, Youtube, Twitter, Instagram, Facebook https://ogusers.com/Forum-Stat-Accounts
Fullz – PHI, Bank/IRA/Stock Trading/Credit Card+
Aged Accounts – Facebook, Instagram, Snapchat
Botnet Proxy services
Cryptocurrency laundering – blending

Cyber Crime Services

DDOS as a service
Tech support scammers
Romance fraud
VoIP fraud
ATM malware – jackpotting
Extortion – PII release, PHI dump, Sextortion, Celebrity Nudes
Cross shipping services
Target list services (email, social media account names)
SIM Swapping
Search Engine Optimization

Cyber Crime Services

Hash cracking services
Domain takeover
Similar domains, Certificate fraud
Spambot
Dark markets – guns, drugs, human trafficking, cheat hardware, hacking hardware
CaaS
Cracked Software, LMS fraud
https://sellcvvdumps.shop/

Cyber Crime Services

CaaS - combolist as a service: https://www.bleepingcomputer.com/news/security/crooks-sell-credentials-using-combolists-as-a-service-model/
new subscriptions offering password dumps updated monthly have started appearing on cracking forums like CrackedTO (TO for Take Over)
Account take over (ATO) actors are in need of new dumps from hacked databases and a seemingly endless stream of infostealer malware and RATs.
Websites like datasense[.]pw also offer CaaS containing passwords dumps for Amazon, Electronic Arts' Origin, Ubisoft's uPlay, Netflix and Steam accounts.
DatabaseHUB also offers CaaS providing daily updated credential lists which can be accessed by customers after buying a token via the crooks' Shoppy-based e-commerce platform. In addition to offering recently stolen passwords, CaaS allows for automation to fuel continuous ATO operations. Combolists are grouped by category such as german, gaming or crypto

Vishing
Smishing
RoboCalls
Cracked Software, LMS fraud

https://sellcvvdumps.shop/ - more than just another carding market, they seem to offer cash out services for money laundering as well

Cyber Crime Services

- At $9, Arcane Stealer V is for now targeted at the lower end of the market, that could change, because the author does make available the raw code for sale too.
- TRT researchers said that he or she sells the malware on their own website and on the Lolzteam site on the Dark Web, and TRT saw several cracked versions available for download on multiple community discussion and file-sharing platforms, like gaming forums and MegaNZ.

Cyber Crime Services

dark.fail is a 'Is this site down for everybody or just me' website for TOR sites.
Dread is a Reddit style forum for discussions about dark markets. There are discussions about which .onion sites trust worthiness
Website listing dark web markets and forums by name and URL:

https://deeponionweb.com/category/news/ - news about dark markets, who got busted and who is a scam

https://deeponionweb.com/category/markets/ - markets in basic categories

https://deeponionweb.com/category/top-markets/ - list of top tier markets like Dream market and Wall Street market

Raid Forums – buy sell data dumps, combo credential lists

XMR.TO allows you to make a bitcoin payment with the strong privacy provided by Monero
Elude.in bitcoin mixer and Monero exchange platform focused on privacy, anonymity, and encryption completely trackless
CoinPayments multi-currency wallets supports more than 700 cryptocurrencies supports storage and use of cryptocurrencies
UAS RDP shop
Proton Mail end to end encrypted email service protected by Swiss privacy law
Empire Market has a CC autoShop where vendors can upload their cards to, there is an optional card checker for buyers to ensure their card is still live upon purchase
Nightmare market – market for buying / selling stolen data and counterfeit consumer goods as well as drugs and a variety of other content
DreamMarket - market for buying / selling stolen data and counterfeit consumer goods as well as drugs and a variety of other content
Tochka Market – market supports buying / selling stolen data as well as lots of other goods

Cyber Crime Services

- According to court documents presented at a case in Germany, in May 2019, the German police discovered a bullet-proof hoster in an old NATO bunker underground in Germany. *The perpetrators were operating a data center in a former NATO bunker in Traben-Trarbach under the name "Cyberbunker" whose sole purpose was to store websites of criminal offenders and to allow criminal activity and attacks. The bunker hosted numerous websites used by internationally active criminals to distribute banned goods such as drugs and fake documents and stolen data, distribute child pornography, and conduct large-scale cyber attacks.*
- *These market place forums and dark web sites were housed in the Cyberbunker*
- *"**Cannabis Road**": sellers of illegal drugs of all kinds. Sold several thousand cannabis products.*
- *"**Wall Street Market**": According to investigations by the Attorney General Frankfurt, the "Wall Street Market" is the second largest marketplace of its kind in the world. In structure, the platform resembled a legitimate e-commerce platform much like Ebay. This platform is said to have handled 250,000 drug trafficking transactions with a sales volume of more than 41 million euros.*
- *The underground forum "**Fraudsters**": The LZC itself investigates the operators of this forum. It is suspected that several thousand narcotics transactions have been processed via this platform.*
- *"**Flight Vamp 2.0**": This marketplace is the largest Swedish Darknet marketplace for illegal sale of narcotics. There are 600 sellers and about 10,000 buyers have been active in the marketplace.*
- *"**orangechemicals**", "**acechemstore**" and "**lifestylepharma**": Through this internet platform, synthetic drugs were distributed throughout Europe in varying quantities and types. Sales transactions in the five-digit range.*
- *Attack on Telekom routers: Also the large-scale attack on approximately one million Telekom routers in the end of November 2016 was steered over a server in the Cyberbunker.*
- *When searched, the Cyberbunker was found to contain over 200 servers with several internet connections and a large sum of cash. 13 people were arrested for operating the Cyberbunker.*

CASHOUT – HOW DO THE BAD GUYS MAKE MONEY?

E-Commerce Fraud

Ransomware Payments

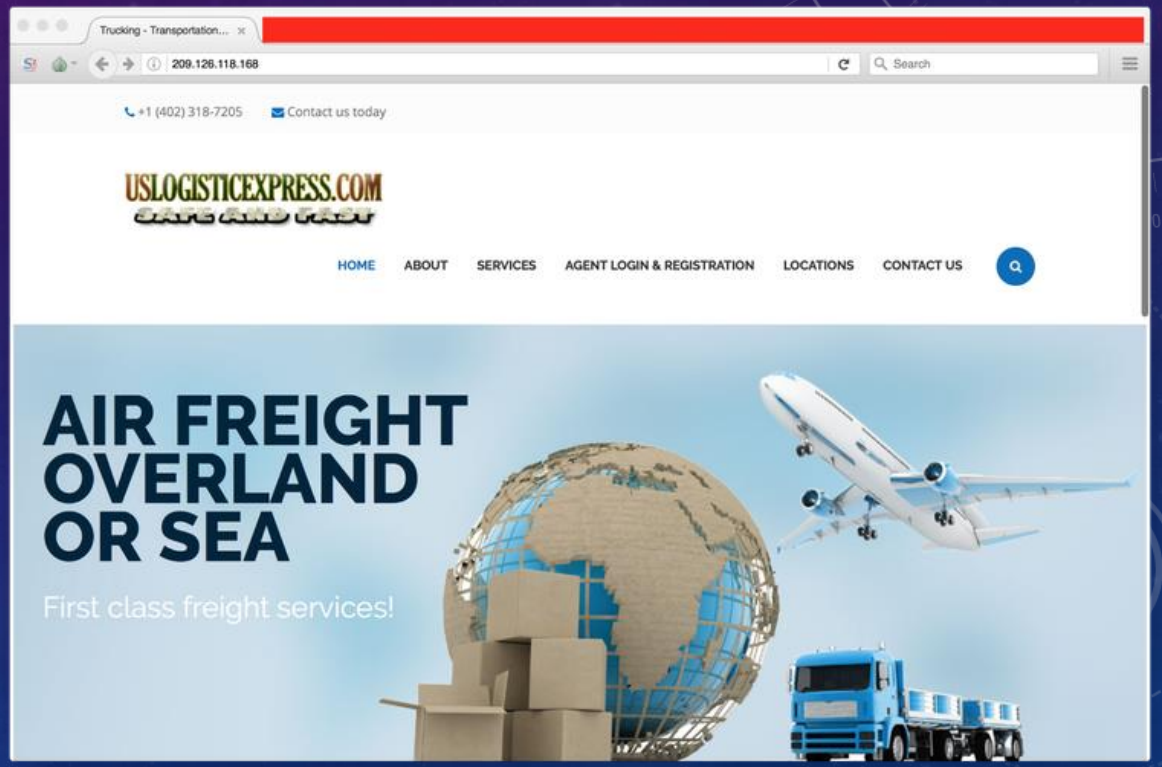
Coin Mining

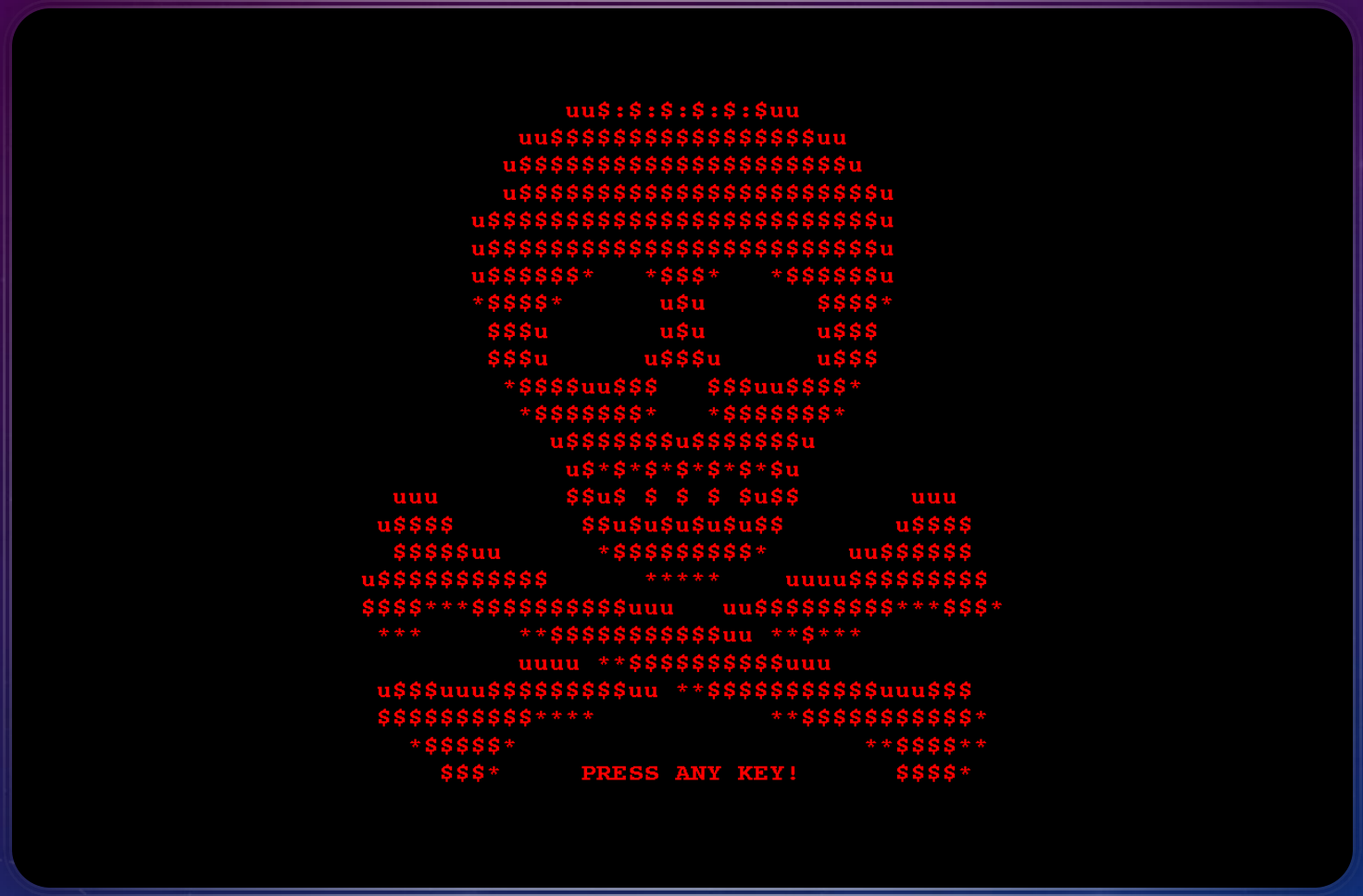
E-COMMERCE FRAUD STOLEN CREDIT/DEBIT CARDS

- MageCart is the most prolific group for stealing credit and debit card information.
- This group is responsible for several high profile breaches recently.
  - Ticketmaster
  - British Airways
  - Newegg
- MageCart is not just one group, but several groups all using skimmers. There is enough overlap and similarities with the groups to be included in the umbrella of magecart.
- The different groups specialize in different functions, some cast a wide net looking for anything open, others seek out high value targets with high volume traffic. Other groups go after 3rd part suppliers (Conversions on Demand and Annex Cloud) to maximize the amount of targets they can breach.
- Skimmer is comprised of javascript embedded into e-commerce pages. Whenever card data was entered into a form, the skimmer would copy the form and send the information to a drop server.
- One way these groups make money is by selling card information through carding shops.

E-COMMERCE FRAUD – RESHIPPING ATTACKS

Once cards information has been resold the next stage in the logistic chain begins. Adds are posted on employment websites for fake companies to recruit “mules” under the disguise of part time reshipping agents. The new employees have to go through a training period and receive several packages. After these packages are received and reshipped the bogus company ceases all communication, withholds promised payment, and leaves the mule to deal with law enforcement





RANSOMWARE PAYMENTS

How do the bad guys make money off Ransomware??? Easy victim pays the ransom……..

Not so simple!

IMPACT OF CYBER INSURANCE ON RANSOMWARE

Cyber insurance is having more of an impact on Ransomware incidents in todays market, consider this good or bad, but it's monetized now.

- In recent Ransomware incident criminals switched to providing an email address vs a ransom amount displayed. They do this to determine if the target caries cyber insurance, if so, the ransom demand goes up.
- Loss of productivity, manufacturing uptime, and access to e-commerce resources are pushing organizations to "pay" ransoms to recover quick as possible. Cyber insurance prefers to pay the ransom, so potentially the insurance provider is not on the hook for loss downtime.

Good or bad cyber insurance is having an impact on todays Ransomware threat landscape.

CRYPTO MINING

- The most popular player on the market is bitcoin, therefore it's becoming increasingly harder to mine. hackers have switched to Monero (XMR).
- A single computer won't help much in mining efforts, so naturally, to make any real money out of mining Moneror, people will need lot of CPU. A lot of CPU powers racks up a considerable electric bill eliminating any profit made. So, instead of using home mining rigs, hackers have figured it's more cost effective to use other peoples CPU.

RISK REDUCTION

When it comes to mitigation advice for the enterprise, they should prevent the preventable by patching and hardening systems, not using defaults

Enterprises also have to do the basics of cyber hygiene and have the ability to recover and be resilient.

Anti fragility is critical, and that's about more than prevention, it's detection, segmentation, back up, it's redundancy and it's recovery.

Preventive measures, such as reviewing vulnerabilities on servers, segmentation and reviewing user access rights, are easy to suggest but evidently harder to implement. Endpoint hardening is cheaper and easier.

Start by identifying the data and systems that are critical for your business to continue to function.

FORMAT NOTES

- Four Sections
- Limit each section to seven minutes
- Develop two to three questions for the audience after each section
- Have five minute Q/A ending for additional questions

POWERSHELL HARDENING RECOMMENDATIONS

1) Enable Powershell logging

2) Use Powershell Constrained Language Mode

3) Disable Powershell 2.0 Engine to prevent down grade attacks in Windows 10

4) Install CVE-2019-0632 important patch to Powershell to fix constrained language mode bypass attack (patched in Feb 2019)

5) Use EDR software that can detect and block powershell abuse

6) Execution Policy Code Signing

DEFENSE IN DEPTH

Best Practices To Prevent Phishing Disasters

- **Implement Technical Controls To Protect End Users:**
  - **Deploy email content filtering as it's 1st line of defense against spam and other malicious emails.**
  - **Enforce email authentication which** uses domain-based message authentication, reporting, and conformance (DMARC) capabilities for anti-spoofing prevention so the security team can detect when incoming emails are using false "from" addresses.
  - Enforce security awareness training
  - Leverage threat intelligence and use the data shared to update your policies and training materials with the latest know

BEST PRACTICES TO PREVENT RANSOMWARE DISASTERS

1. Have good back up strategy. Also know what type of back up your organization is running as you do now want to backup the ransomware.
2. Keep your firewalls policies and antivrus uptodate as they are the first line of defense.
3. Consider a managed detection response service . MDR monitors everything from our network to endpoints to cloud services like Office 365, giving us a holistic view. It has also reduced the number of false positive alerts we've had to deal with.
4. Have a good incident response plan that includes everyone from Legal to IT to HR.

BACK TO BASICS PREVENTION