HACKING-AS-A-SERVICE: BECOMING AN APT IS EASIER THAN EVER!

- Will | @BushidoToken
- Security Researcher
- CTI Analyst
- OSINT Investigator
- Volunteer
- Community Staff

ncptf
national child protection task force

WANTED BY THE FBI

"THE BEER FARMERS"

Conspiracy to Commit an Offense Against the United States; False Registration of a Domain Name; Conspiracy to Commit Wire Fraud; Wire Fraud; Intentional Damage to Protected Computers; Aggravated Identity Theft

>> OBLIGATORY_INTRO_SLIDE <<

github.com/BushidoUK

bushidotoken.net

@BushidoToken

- Who is this talk for?
  - Students and Professionals
- Terminology & Acronyms
  - Malware, Exploit, Threat Actor
  - APT, OST, 0day, OSINT
- This this is being recorded ⏯
- The slides will also be available on my GitHub

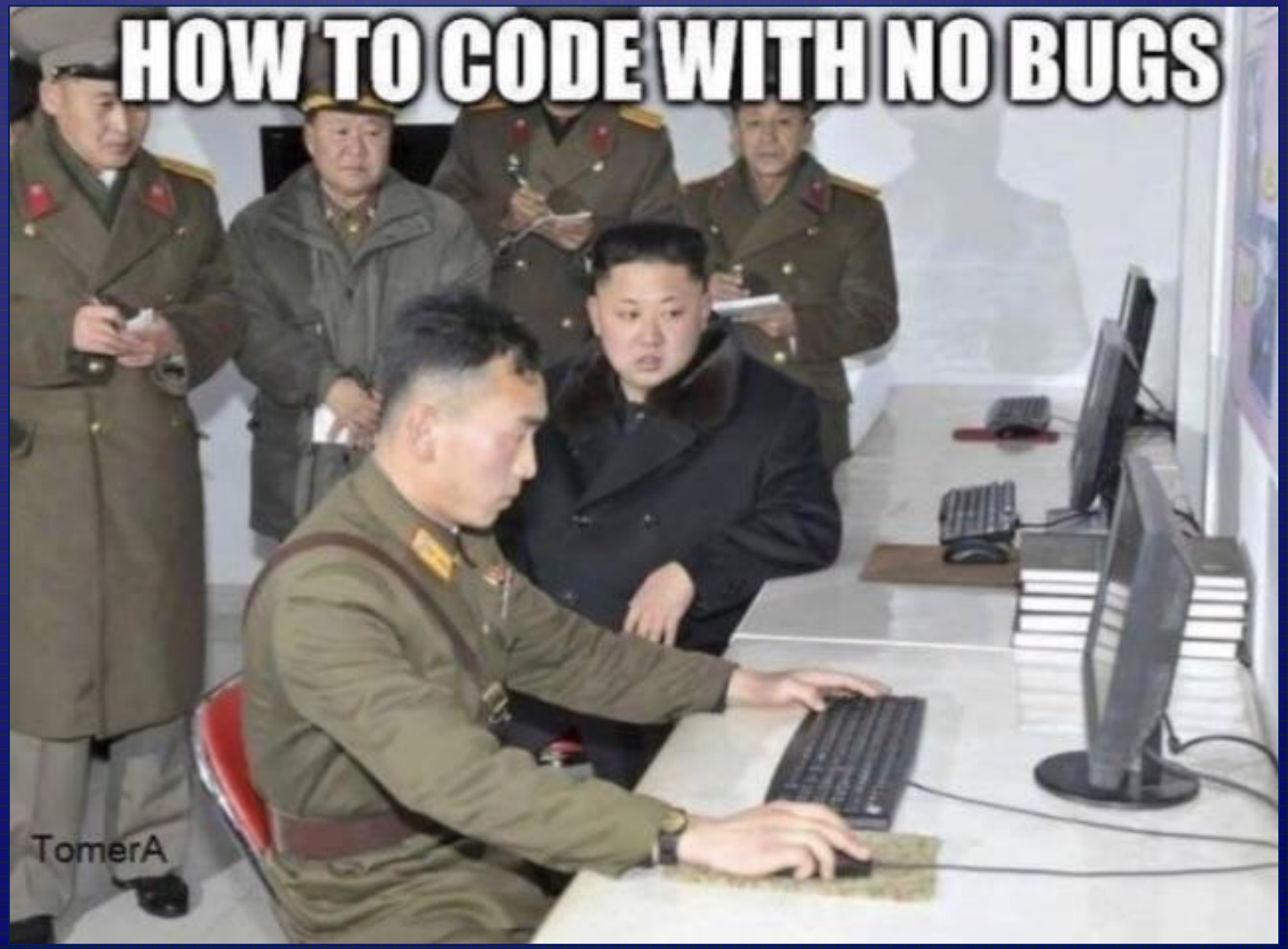
WHAT IS AN APT?

- Nobelium - Russian Foreign Intelligence – SVR
  - SolarWinds supply-chain attack
  - Think Tanks & The Whitehouse

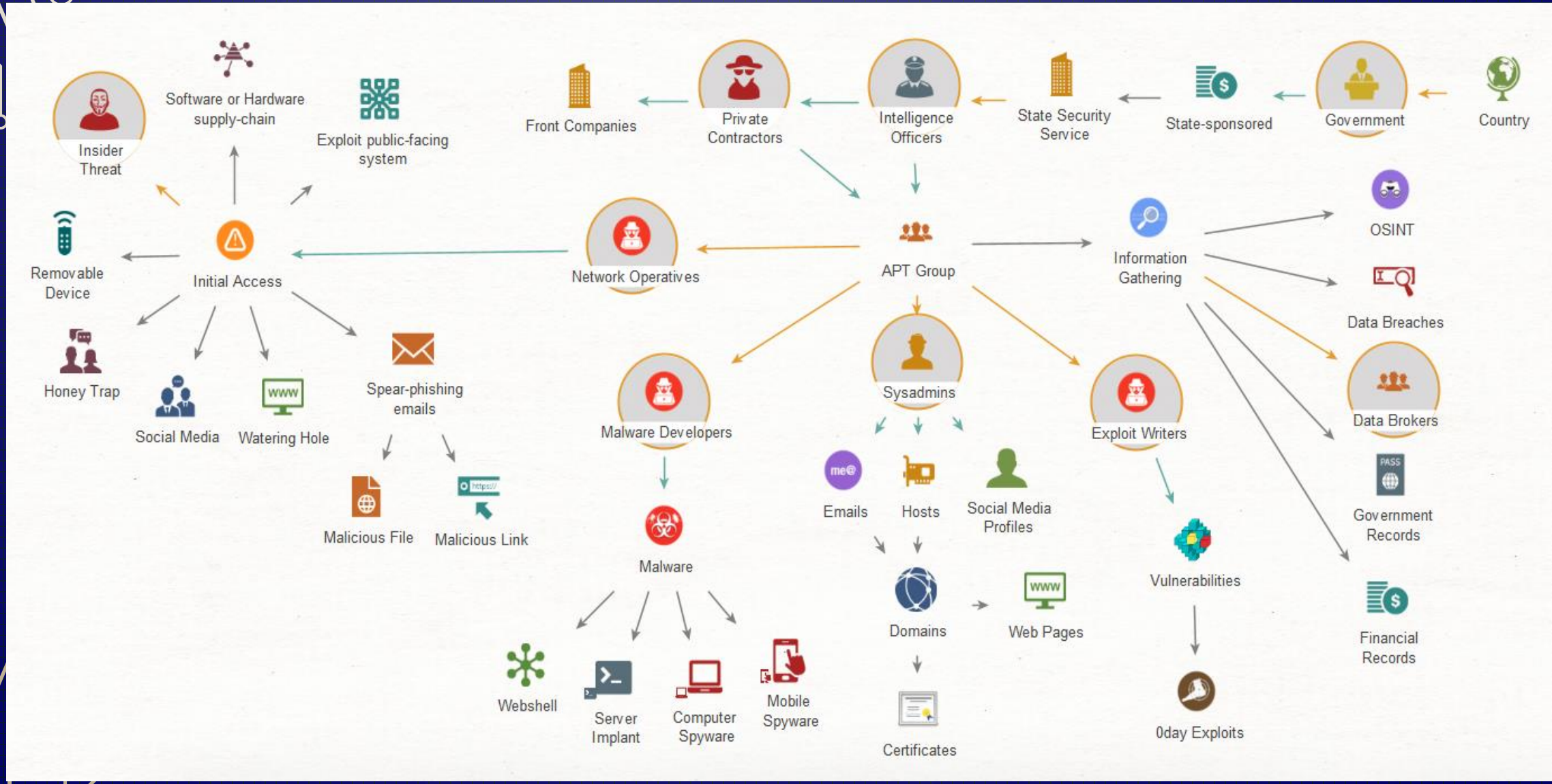
- FancyBear – Russian Military Intelligence – GRU
  - Hack & Leak: DNC, WADA, CyberBerkut
  - Bundestag & Storting

- Sandworm – Russian Military Intelligence – GRU
  - ICS: BlackEnergy, Industroyer/CrashOverride
  - NotPetya, BadRabbit, OlympicDestroyer ransomware

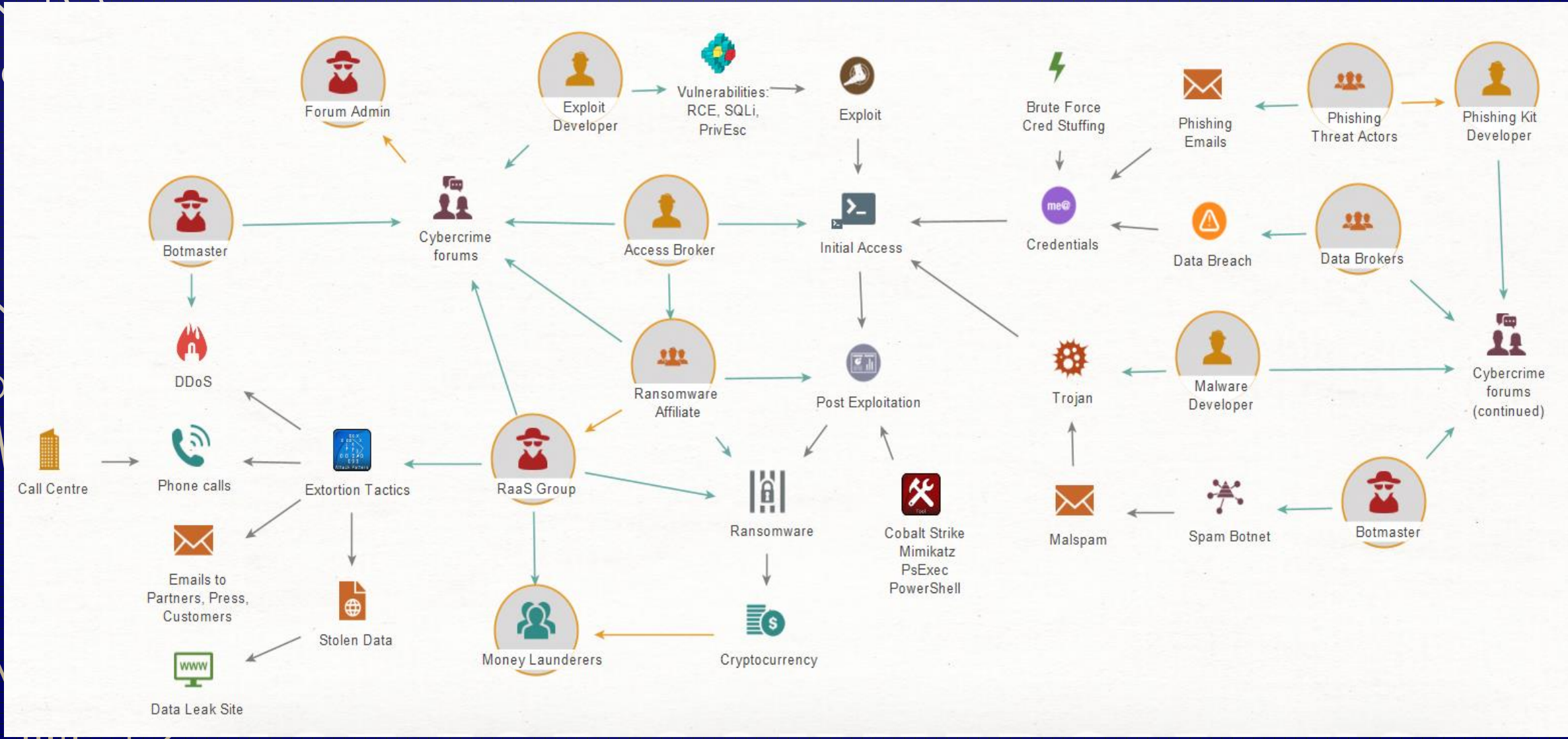
FASTEST WAY TO BECOME AN APT



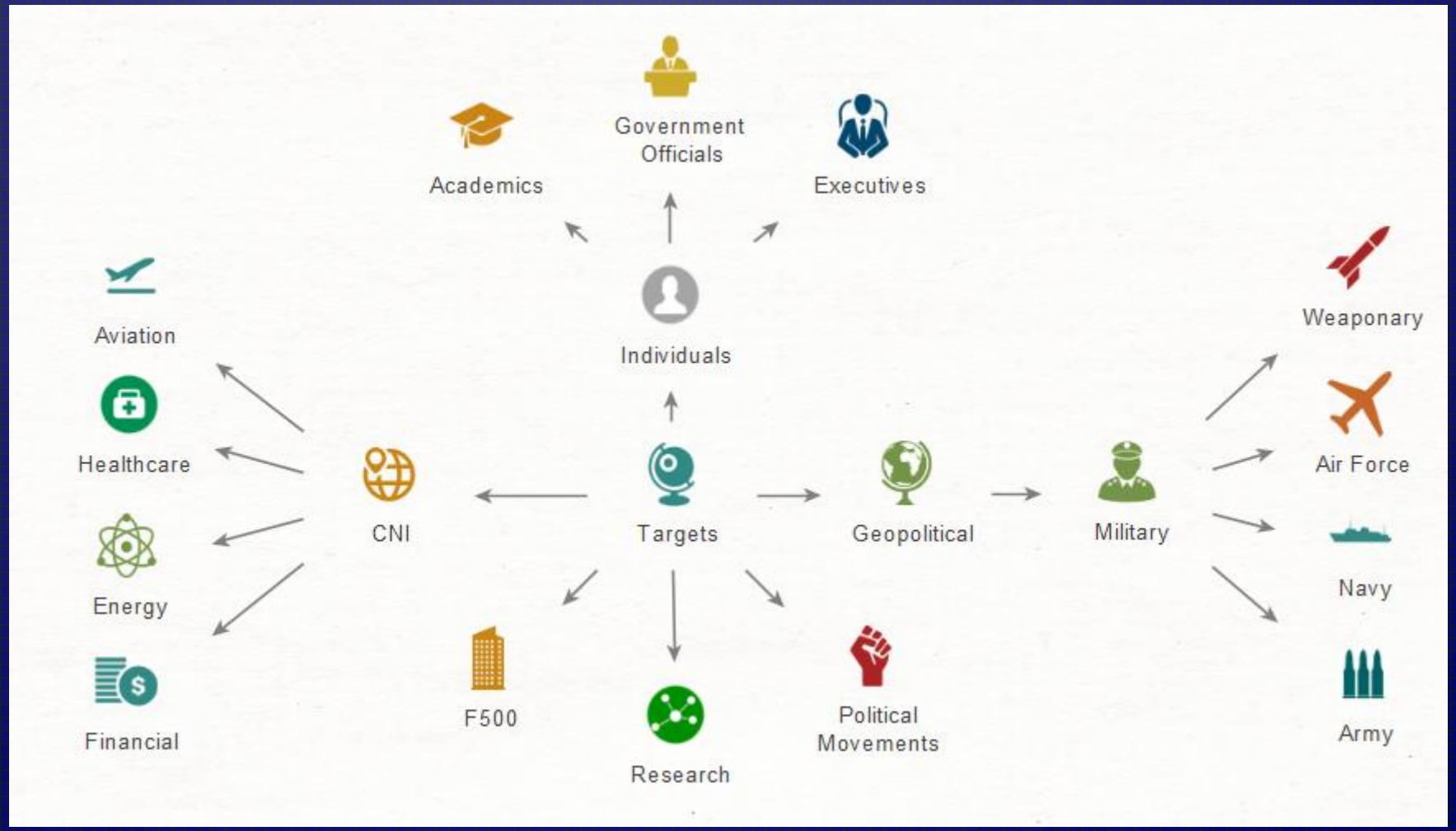
ESPIONAGE GROUPS



CYBERCRIME GROUPS



APT TARGETS


Academics
Government Officials
Executives
Aviation
Individuals
Weaponary
Healthcare
Air Force
CNI
Targets
Geopolitical
Military
Energy
Navy
F500
Political Movements
Financial
Research
Army

WHAT IS A MERCENARY APT?

- Groups – CostaRicto, Bahamut, DarkBasin, DeathStalker, Project Raven, NSO Group, Candiru, Hacking Team, Gamma Group

- Customers – Governments, Law Enforcement, Counter Terrorism, Conglomerates

- Tradecraft – OSINT, HUMINT, SIGINT, 0day exploits, malware developers, data acquisition, darknet markets, phishing, social engineering, spyware, persistent access, detection evasion

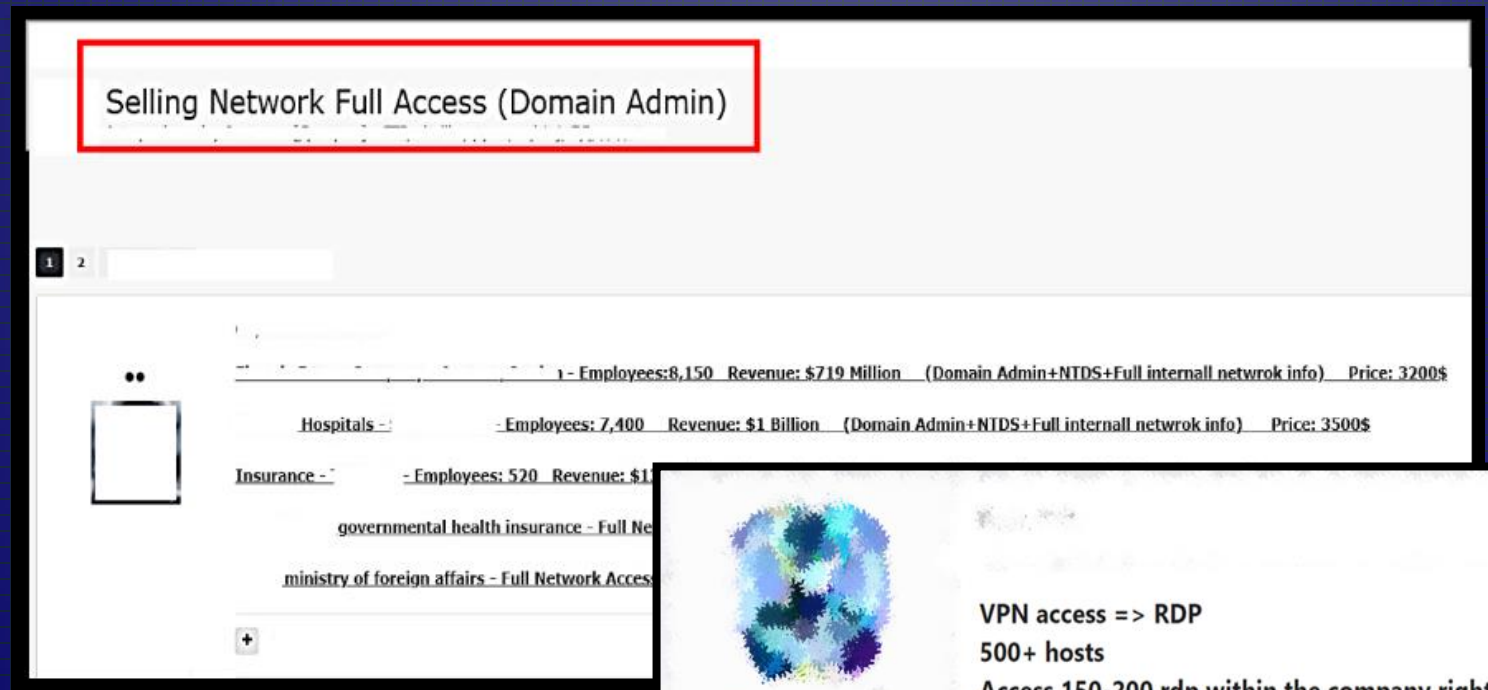
MERCENARY APT CUSTOMERS

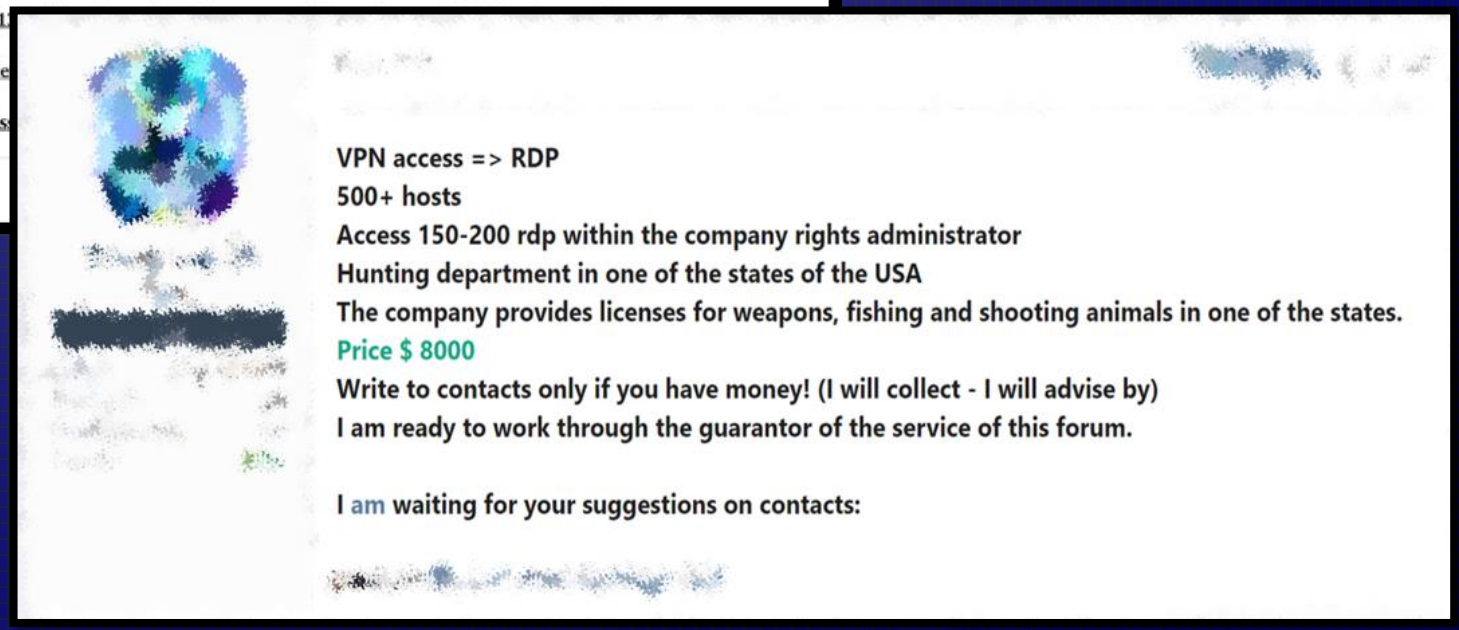
- #ExxonKnew – DarkBasin was hired to target American activists campaigning against ExxonMobil for withholding information about the climate crisis
- Mexico's soda tax – Public health scientists and two directors of Mexican NGOs working on obesity and soda consumption were targeted with NSO Group's Pegasus mobile spyware
- Jamal Khashoggi – a Washington Post columnist was assassinated at the Saudi Arabian embassy in Istanbul and NSO's spyware was found on the phones of people close to Khashoggi before and after his death
- Project Raven – ex-NSA employees established a company called Dark Matter in the UAE to help spy for the monarchy on dissidents, rival leaders, and journalists

PREPARATION

- Finance
- Personas
- Information Gathering
- Initial Access
- Malware
- Infrastructure
- Exploit Acquisition
- Recruiting Hackers
- Deployment

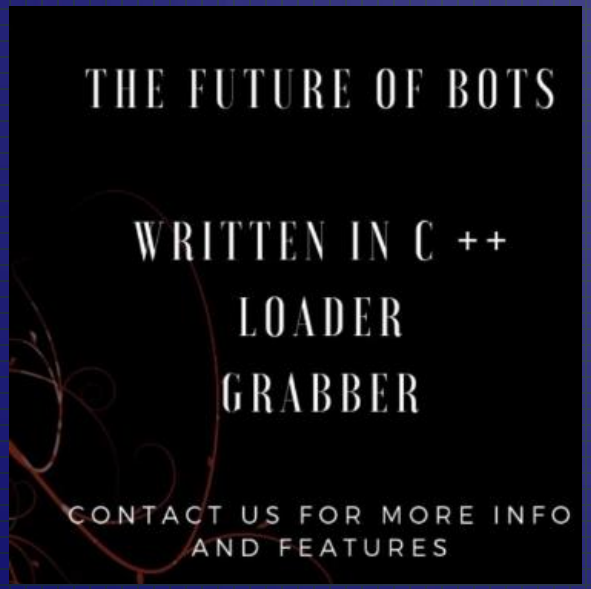
INITIAL ACCESS





MALWARE-AS-A-SERVICE

LOADER



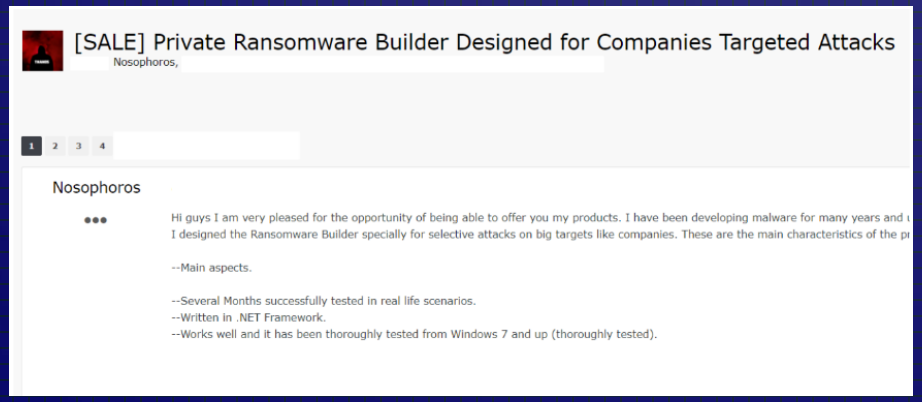
Prices:

--Lifetime building and updates: 2500 US$ in btc.
--One month usage with free updates: 800 US$ in btc.

What you get:

--Usage Video Tutorial.
-- Private Ransomware Builder.
--Free additional obfuscation utilities in case you need them.

CRYPTER



RANSOMWARE

Prices:

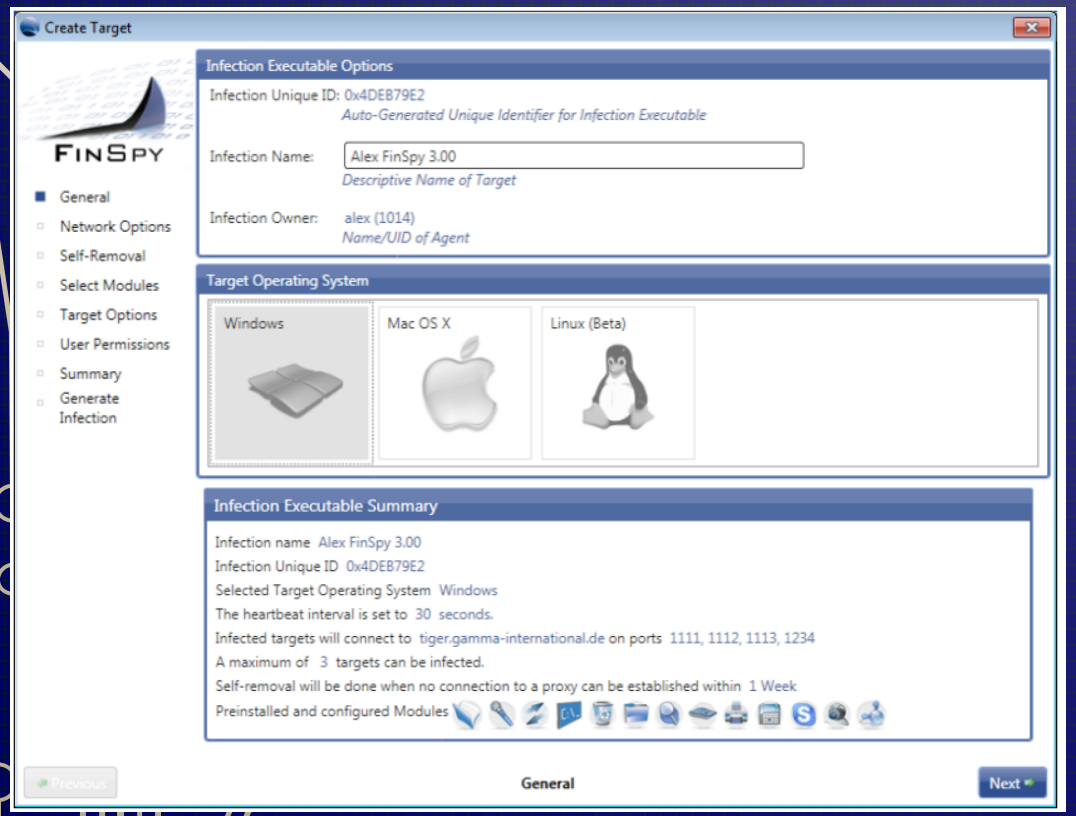
Basic Plan 1 Month Builder access: 500 usd in BTC.
Pro Plan 1 month Builder access: 800 usd in BTC.
Unlimited: 3000 usd in BTC.

All plans have free automatic updates of the builder during its usage time.
All created clients do not expire.

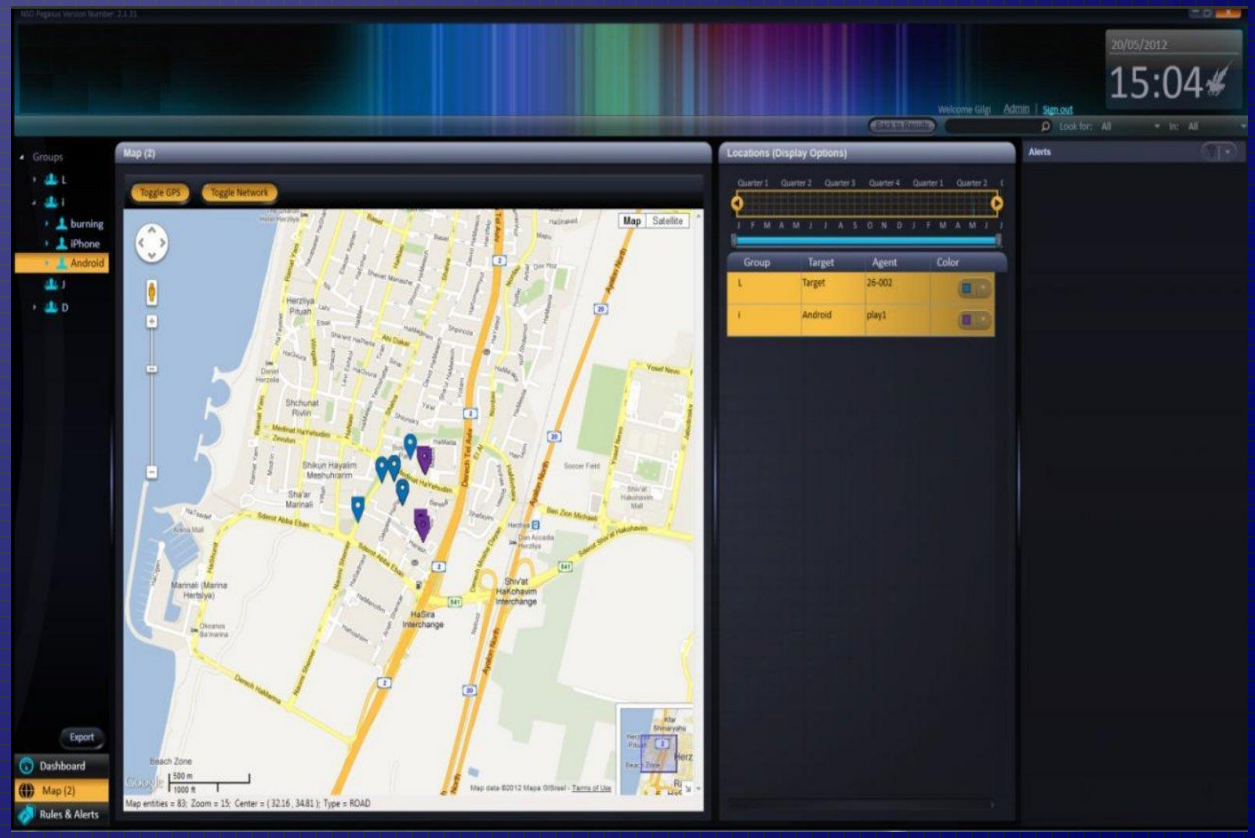
PAYMENT PLANS

CUSTOM SPYWARE TOOLS

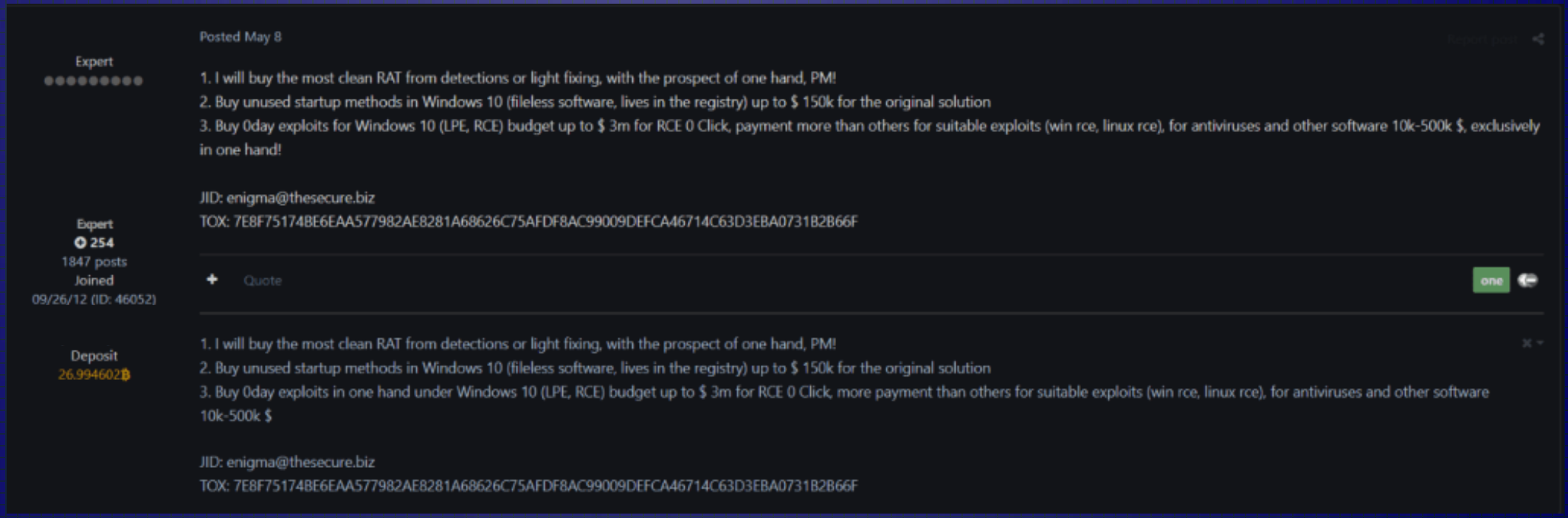
FINSPY



PEGASUS



EXPLOIT ACQUISITION



Posted May 8

Expert

1. I will buy the most clean RAT from detections or light fixing, with the prospect of one hand, PM!
2. Buy unused startup methods in Windows 10 (fileless software, lives in the registry) up to $ 150k for the original solution
3. Buy 0day exploits for Windows 10 (LPE, RCE) budget up to $ 3m for RCE 0 Click, payment more than others for suitable exploits (win rce, linux rce), for antiviruses and other software 10k-500k $, exclusively in one hand!

JID: enigma@thesecure.biz
TOX: 7E8F75174BE6EAA577982AE8281A68626C75AFDF8AC99009DEFCA46714C63D3EBA0731B2B66F

Expert
254
1847 posts
Joined
09/26/12 (ID: 46052)

Quote

one

Deposit
26.994602

1. I will buy the most clean RAT from detections or light fixing, with the prospect of one hand, PM!
2. Buy unused startup methods in Windows 10 (fileless software, lives in the registry) up to $ 150k for the original solution
3. Buy 0day exploits in one hand under Windows 10 (LPE, RCE) budget up to $ 3m for RCE 0 Click, more payment than others for suitable exploits (win rce, linux rce), for antiviruses and other software 10k-500k $

JID: enigma@thesecure.biz
TOX: 7E8F75174BE6EAA577982AE8281A68626C75AFDF8AC99009DEFCA46714C63D3EBA0731B2B66F

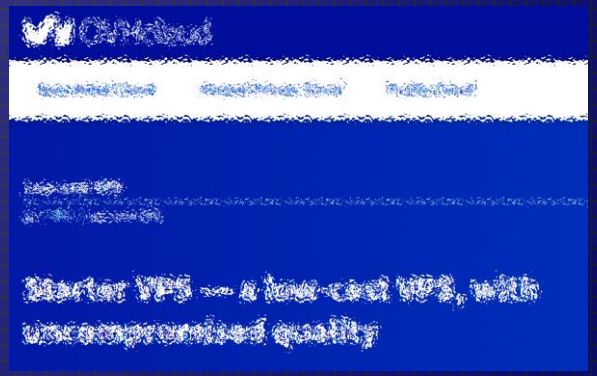
"Buy 0day exploits for Windows 10 (LPE, RCE) budget up to $3m for RCE 0 click, payment more than others for suitable exploits (win rce, linux rce), for antivirus, and other software 10k-500k $"

INFRASTRUCTURE

C&C

VPN

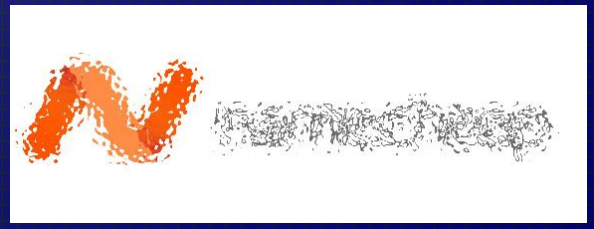
VPS



CERTS

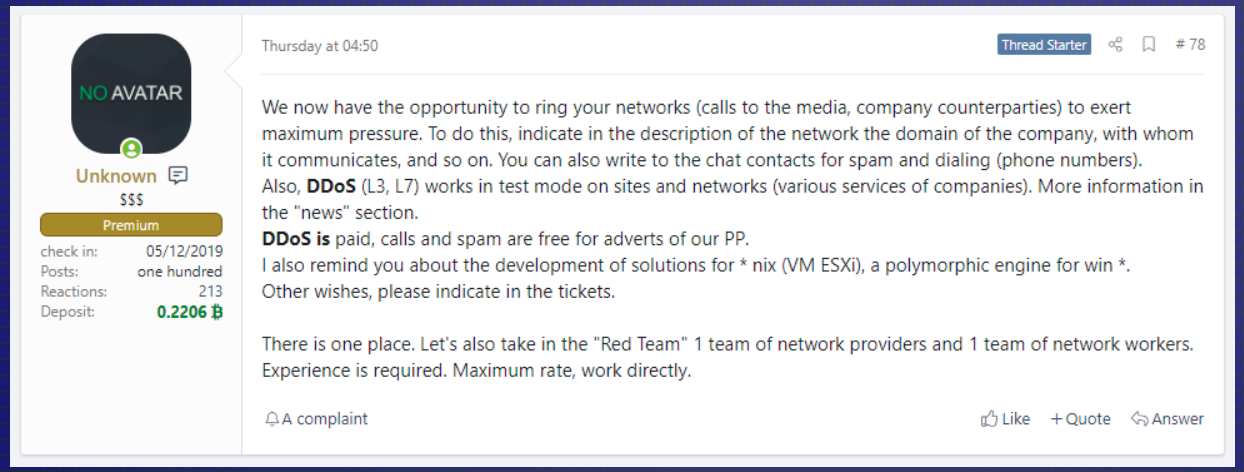
HOSTS

DOMAINS



ACQUIRING HACKERS

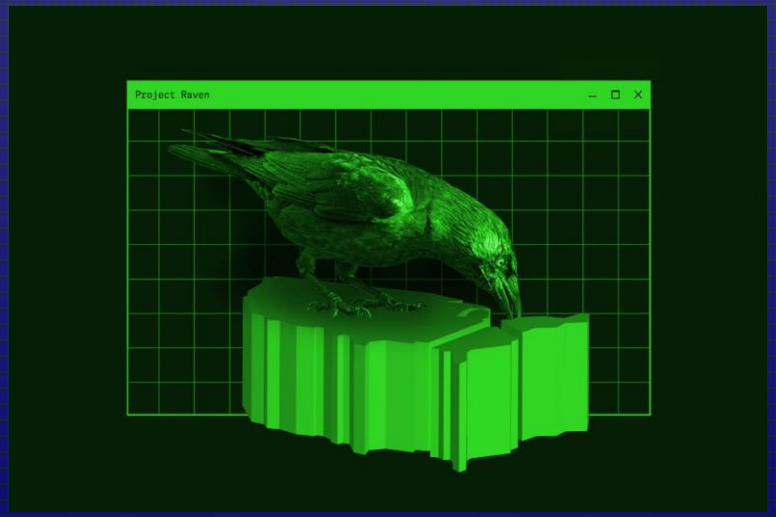
REVIL



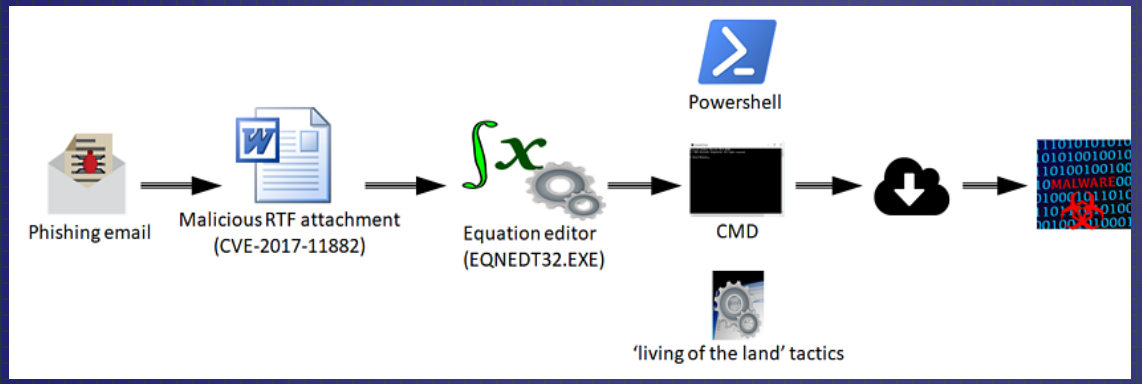
MSS

FIN7

NSA

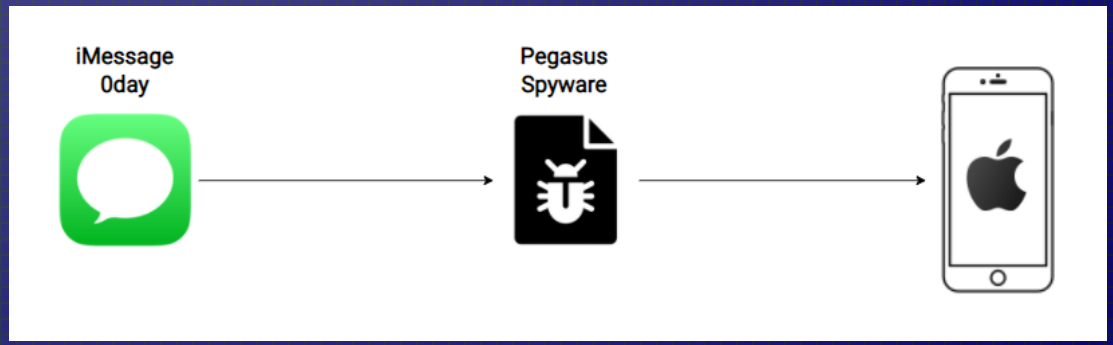


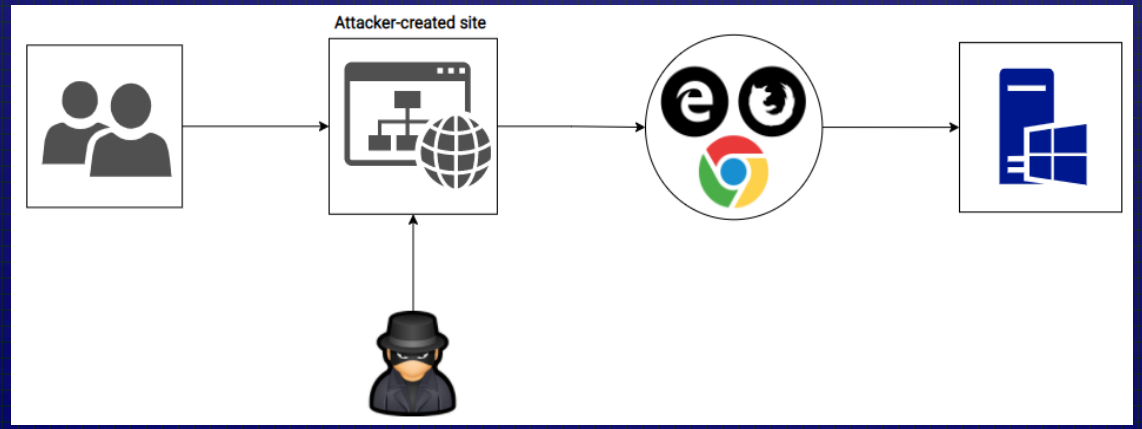
DEPLOYMENT



EMAIL PHISHING

MOBILE EXPLOIT



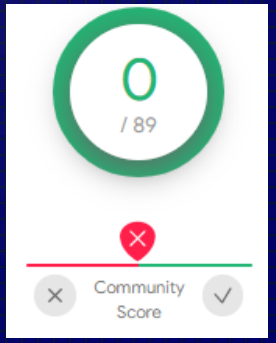


WATERING HOLE

PROS VS CONS

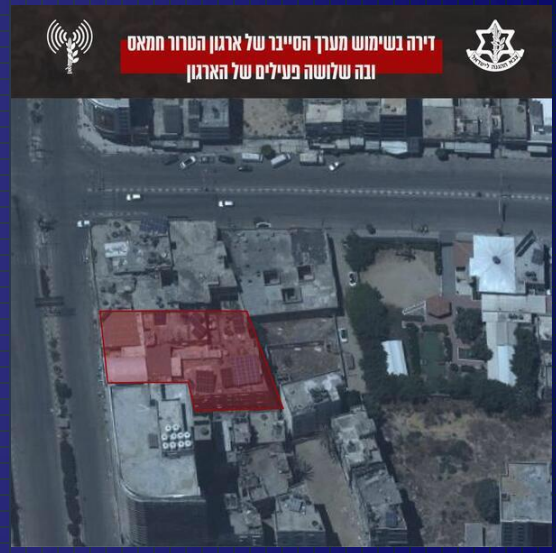
PROS:

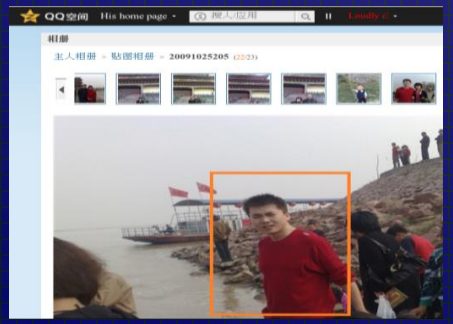
- Acquire sensitive data and secrets
- Make Millions of $$$
- Become a National Hero
- Go completely unnoticed for years
- Have Talks, Blogs, & Podcasts made about you



CONS:

- Bombed by Israel
- Indicted by the DOJ
- Can’t leave the country or go on holidays
- Doxed by IntrusionTruth
- Get hacked yourself (PhineasFisher or ShadowBrokers)
- Made fun of by researchers in Talks, Blogs, & Podcasts



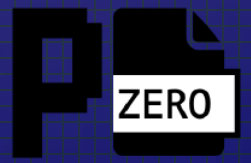


OPPOSITION

RESEARCHERS

INTELLIGENCE AGENCIES & LAW ENFORCEMENT

VENDORS



SIDE AFFECTS

- 0days are horded, nothing gets patched
- Your Malware & 0days get leaked
- WannaCry or NotPetya
- Colonial Pipeline or Irish HSE
- Assassinations
- Imprisonment

SECURITY NIHILISM?

OMFG?!

- “Sophisticated” APTs
- “State-sponsored”
- 0day vulnerabilities
- Undetectable malware
- Unremovable malware
- 24/7 attacks
- $$$

YES WE CAN

- Patch Management
- 2FA/MFA
- Password Manager
- EDR/AV
- Distrust Email Attachments
- Confirm identities
- Avoid unknown software
- Only use trusted sources
- Use a sandbox / VM
- Turn off unused features
- Make backups
- Replace EoL equipment
- Threat Intelligence

THANK YOU

github.com/BushidoUK

Twitter.com/BushidoToken

bushidotoken.net

REFERENCES

- https://www.youtube.com/watch?v=ZDHHGZlEfsQ
- https://adversary.crowdstrike.com/en-US/adversary/cozy-bear/
- https://www.crowdstrike.com/blog/who-is-fancy-bear/
- https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html
- https://www.theguardian.com/technology/2020/jun/11/exxon-hack-for-hire-climate-activists-campaign
- https://citizenlab.ca/2017/02/bittersweet-nso-mexico-spyware/
- https://www.theguardian.com/world/2021/jul/18/nso-spyware-used-to-target-family-of-jamal-khashoggi-leaked-data-shows-saudis-pegasus
- https://www.reuters.com/investigates/special-report/usa-spying-raven/
- https://blog.cyble.com/2021/07/06/threat-actor-seeking-private-0-day-1-million-deposited-in-a-popular-cybercrime-marketplace/
- https://s3.documentcloud.org/documents/4599753/NSO-Pegasus.pdf
- https://netzpolitik.org/wp-upload/0F28548C.pdf