



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

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





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 <<

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



github.com/BushidoUK

bushidotoken.net

@BushidoToken

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



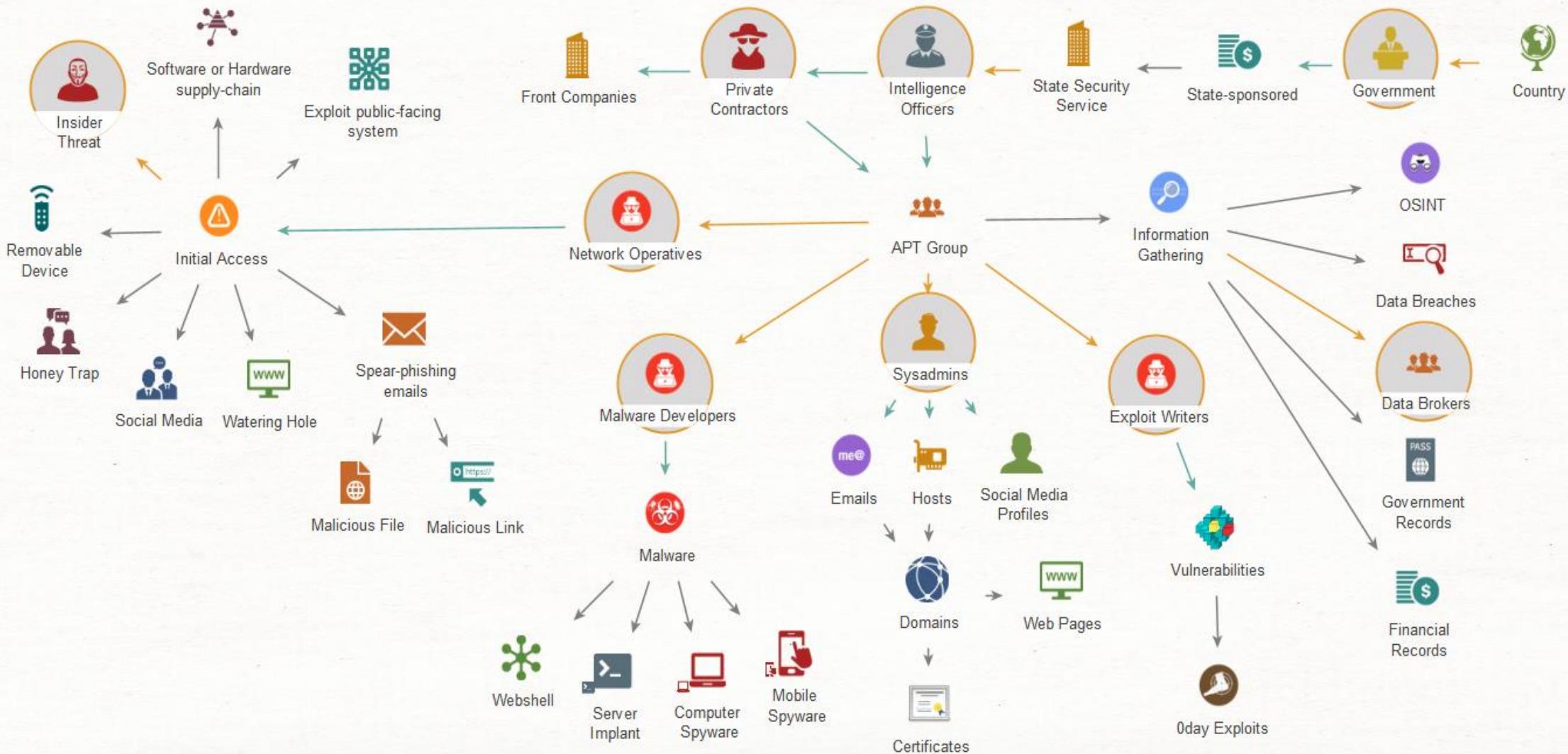
- Sandworm – Russian Military Intelligence – GRU
 - ICS: BlackEnergy, Industroyer/CrashOverride
 - NotPetya, BadRabbit, OlympicDestroyer ransomware



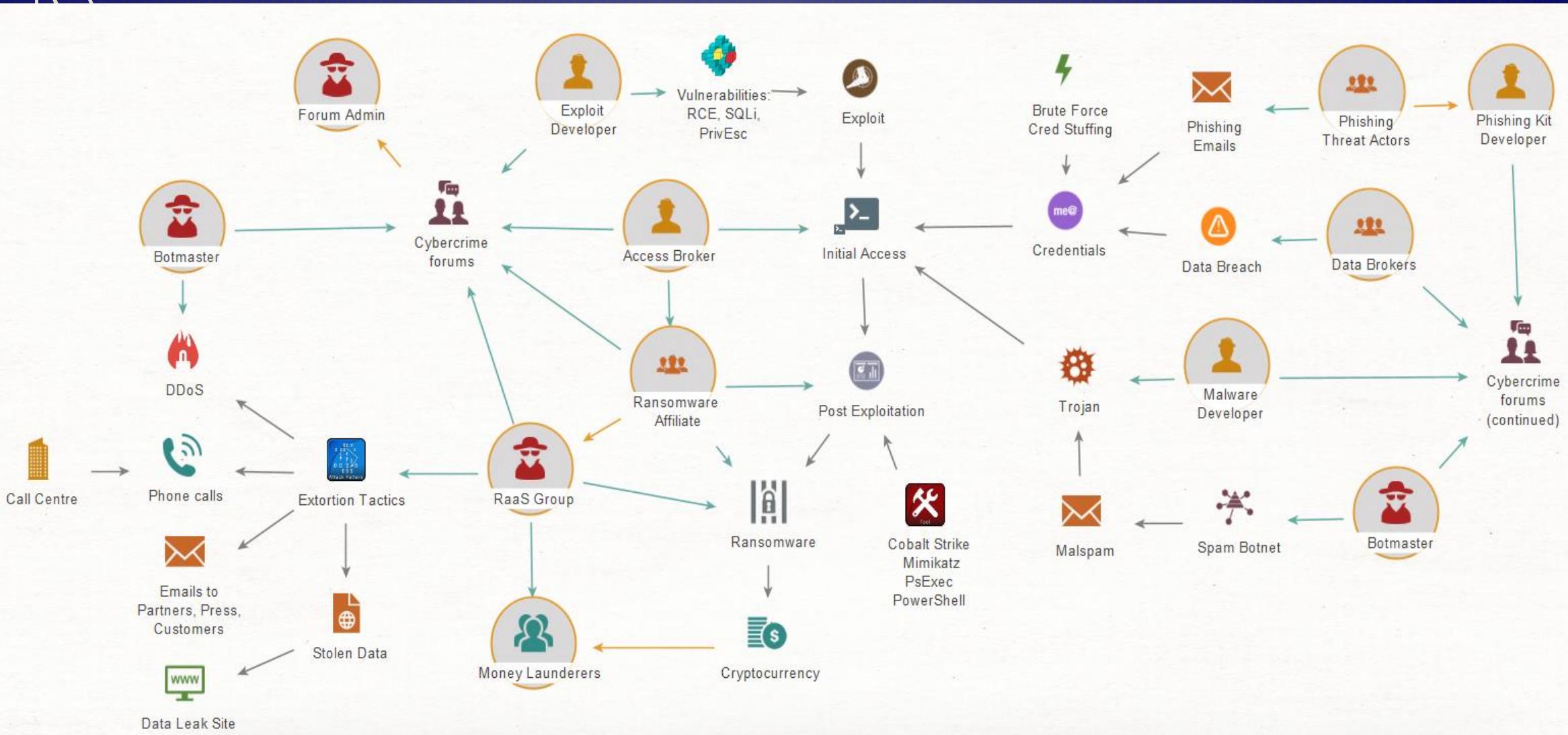
FASTEST WAY TO BECOME AN APT



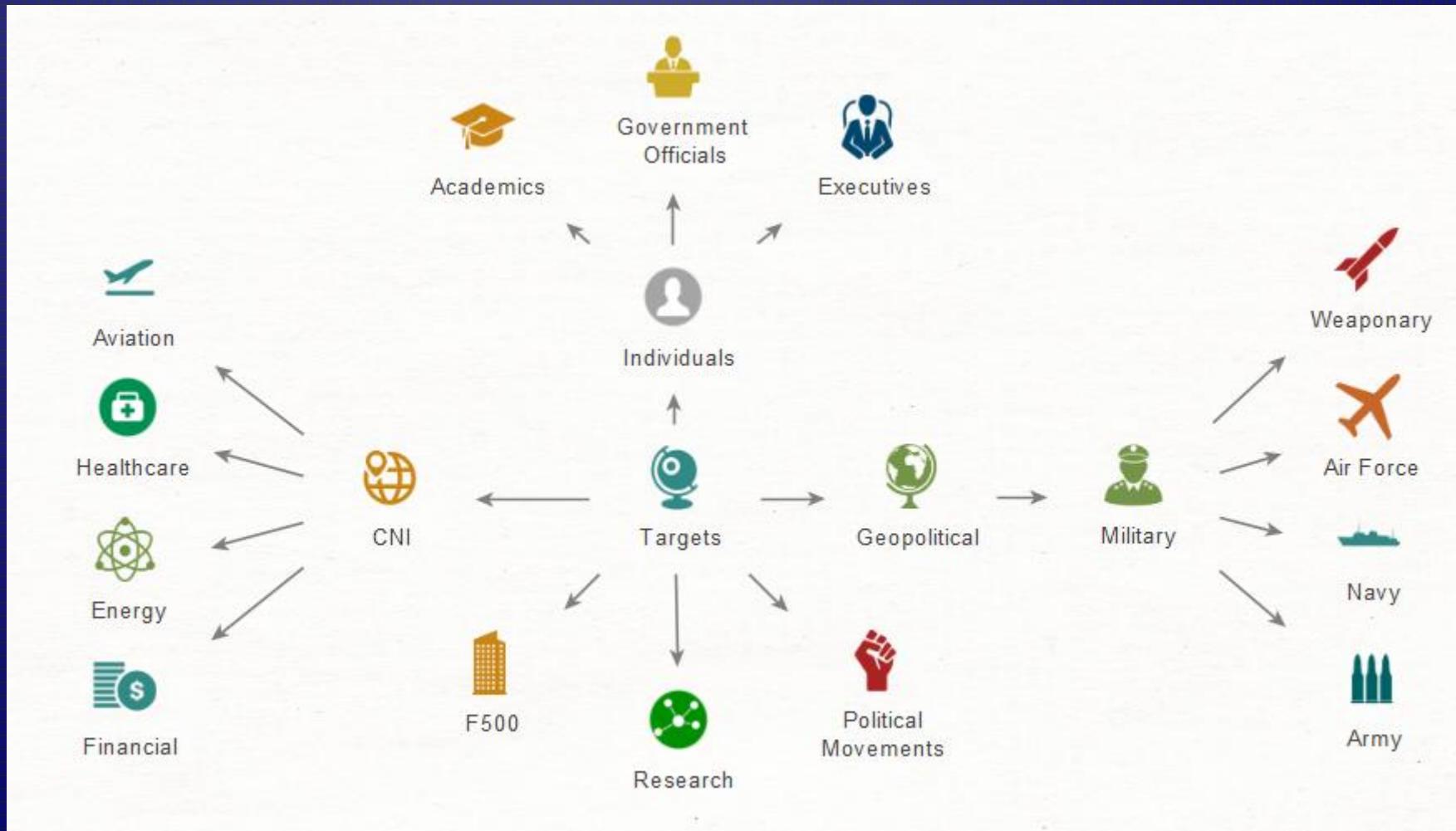
ESPIONAGE GROUPS



CYBERCRIME GROUPS



APT TARGETS





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

Selling Network Full Access (Domain Admin)

1 2

1 - Employees: 8,150 Revenue: \$719 Million (Domain Admin+NTDS+Full internal network info) Price: 3200\$

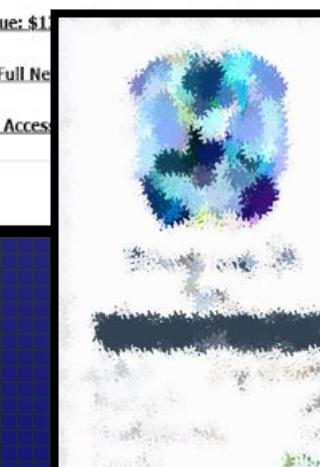
Hospitals - Employees: 7,400 Revenue: \$1 Billion (Domain Admin+NTDS+Full internal network info) Price: 3500\$

Insurance - Employees: 520 Revenue: \$1.5 Billion (Domain Admin+NTDS+Full internal network info) Price: 3000\$

governmental health insurance - Full Network Access

ministry of foreign affairs - Full Network Access

+



VPN access => RDP

500+ hosts

Access 150-200 rdp within the company rights administrator

Hunting department in one of the states of the USA

The company provides licenses for weapons, fishing and shooting animals in one of the states.

Price \$ 8000

Write to contacts only if you have money! (I will collect - I will advise by)

I am ready to work through the guarantor of the service of this forum.

I am waiting for your suggestions on contacts:

MALWARE-AS-A-SERVICE

LOADER

THE FUTURE OF BOTS

WRITTEN IN C ++
LOADER
GRABBER

CONTACT US FOR MORE INFO
AND FEATURES

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

SILVER-CRYPTER

- NET AND NATIVE APPLICATIONS
- AUTOMATIC UPDATES
- SUPPORTS DRAG&DROP AND CONTEXTUAL HELP
- INCLUDES AN INTELLIGENT ENCRYPTION COUCH
 - PROCESS INJECTION INCLUDING RANDOM INJECTION
- UNIQUE STUB GENERATOR
- MELTING
- SUPPORTS SIMPLE ENCRYPTION, LOADERS CREATION (ADVANCED LOADERS)
- WINDOWS DEFENDER DISABLER AND USB SPREADING)
- FUD WORD AND EXCEL MACROS, ALL IN ONE TOOL
 - SHORTCUT CREATOR
- FILE SPOOFER & SIGNATURE STEALER
- SIMPLE AND ADVANCED OBFUSCATION
 - COMPRESSION ENGINE
- CUSTOMIZABLE ELEVATION REQUEST

1 MONTH
80\$

3 MONTH
200\$

1 YEAR
500\$



[SALE] Private Ransomware Builder Designed for Companies Targeted Attacks

Nosophoros,

Nosophoros

...

Hi guys I am very pleased for the opportunity of being able to offer you my products. I have been developing malware for many years and I designed the Ransomware Builder specially for selective attacks on big targets like companies. These are the main characteristics of the pr...

--Main aspects.

--Several Months successfully tested in real life scenarios.

--Written in .NET Framework.

--Works well and it has been thoroughly tested from Windows 7 and up (thoroughly tested).

RANSOMWARE

Prices:

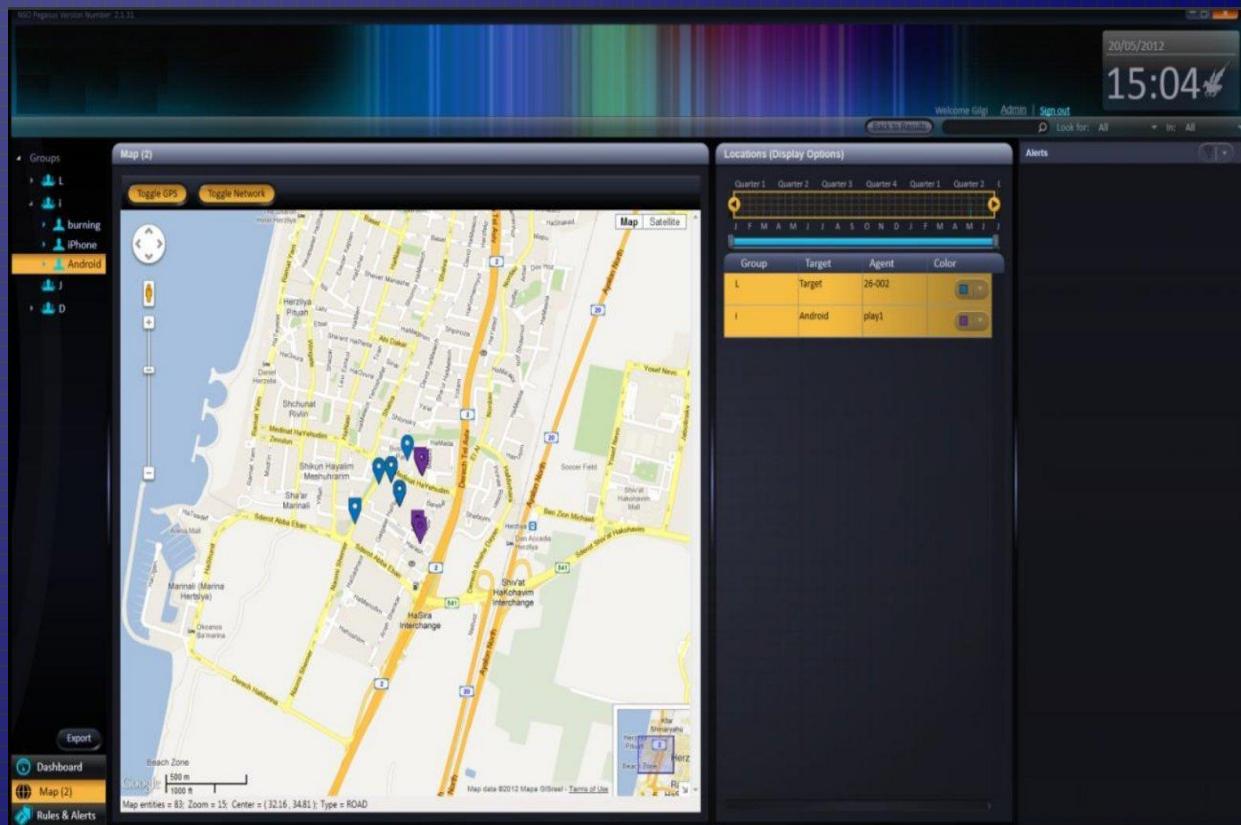
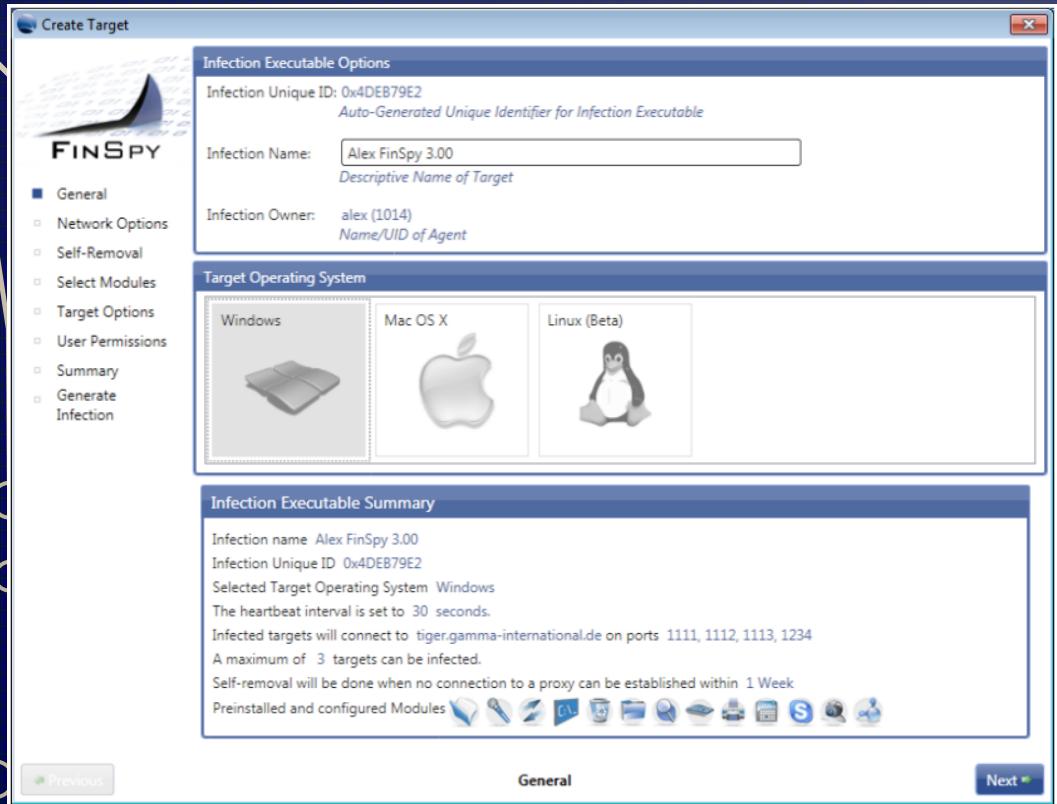
- Basic Plan 1 Month Builder access: 500 usd in BTC.
- Pro Plan 1 month Builder access: 800 usd in BTC.
- Unlimited: 3000 usd in BTC.

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

JID: enigma@thesecure.biz
TOX: 7E8F75174BE6EAA577982AE8281A68626C75AFDF8AC99009DEFCA46714C63D3EBA0731B2B66F

+

Quote

Report post

one

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

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 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 \$, exclusively in one hand!

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 antivirus 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



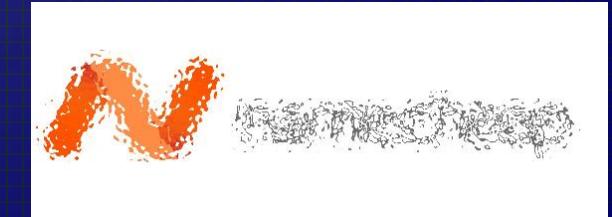
CERTS



HOSTS



DOMAINS



ACQUIRING HACKERS

MSS

REVIL

Thursday at 04:50

Thread Starter # 78

We now have the opportunity to ring your networks (calls to the media, company counterparts) to exert maximum pressure. To do this, indicate in the description of the network the domain of the company, with whom it communicates, and so on. You can also write to the chat contacts for spam and dialing (phone numbers). Also, **DDoS** (L3, L7) works in test mode on sites and networks (various services of companies). More information in the "news" section.

DDoS is paid, calls and spam are free for adverts of our PP.

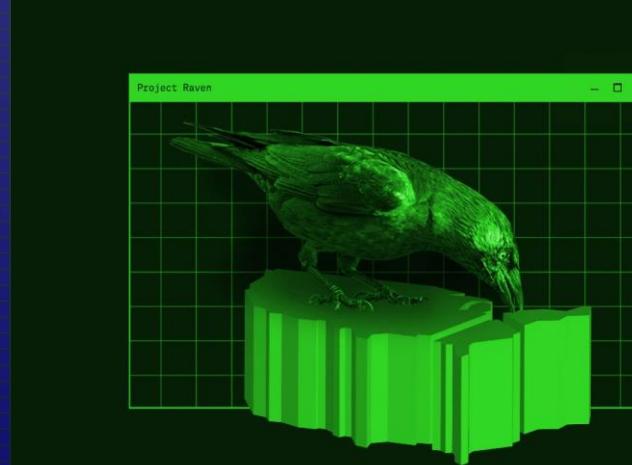
I also remind you about the development of solutions for * nix (VM ESXi), a polymorphic engine for win *. Other wishes, please indicate in the tickets.

There is one place. Let's also take in the "Red Team" 1 team of network providers and 1 team of network workers. Experience is required. Maximum rate, work directly.

A complaint Like + Quote Answer



FIN7



NSA

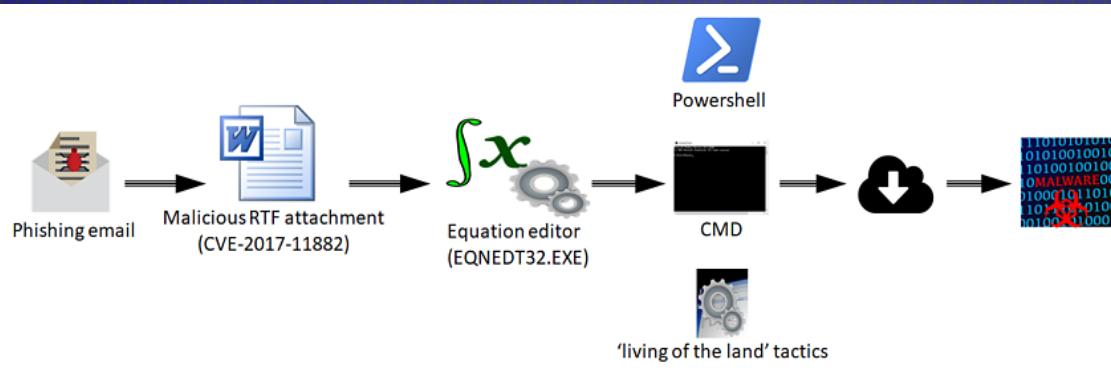
(122) On or about May 29, 2018, defendant DING XIAOYANG was presented an award from the MSS for young leaders in the organization while he was overseeing computer hacking and theft of data conducted by Hainan Xiandun, as depicted in the following photograph:



What is the Hainan Xiandun
Technology
Development Company?

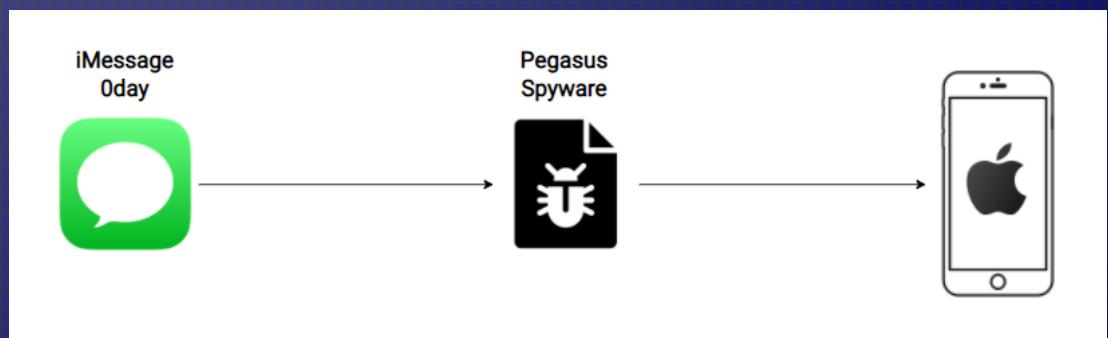
intrusiontruth in Hainan | January 9, 2020 | 1,172 Words

DEPLOYMENT

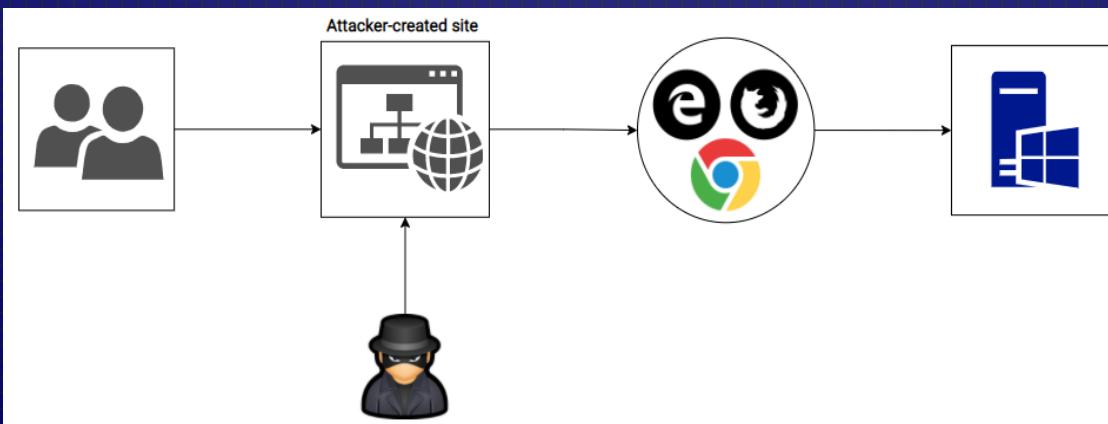


EMAIL PHISHING

MOBILE EXPLOIT



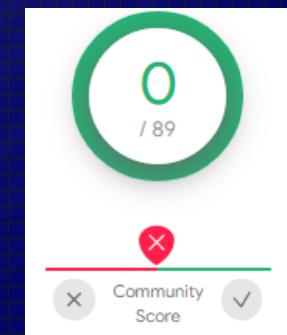
WATERING HOLE



PROS VS CONS

PROS:

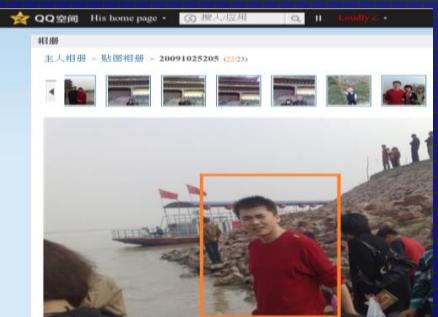
- Acquire sensitive data and secrets
- Make Millions of \$\$\$
- Become a National Hero
- Go completely unnoticed for years
- Have Talks, Blogs, & Podcasts made about you





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



bgld1r.a-fixled.sanchare
bgld1r.a-fixled.sanchare
bj02.cwn.cc_2022_08_24_18_11
bj02.cwn.cc_2022_08_25_10_30
dproxy1.threentech.com_2022_08_25_10_30
dn20.bijep.edu.cn_2022_08_25_10_30
dns2.net.ti_215.140.19
doors.co.kr_211.43.193.
enterprise.telesat.com.co_2022_08_25_10_30
coli.egyptonline.com_2022_08_25_10_30
dn33.npic.ac.cn_168.16
ganbero3.cs.
gate.techno-
hubko.jp_2022_08_25_10_30
lws11.ru_2022_08_25_10_30
kccst.
knowns.
serv.k
lahle.
lahle.ltr
m0-e.san.
n0-e.san.



NSA's Target List Leaked!



OPPOSITION

RESEARCHERS



INTELLIGENCE AGENCIES
&
LAW ENFORCEMENT



VENDORS



SIDE AFFECTS

- 0days are hoarded, 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

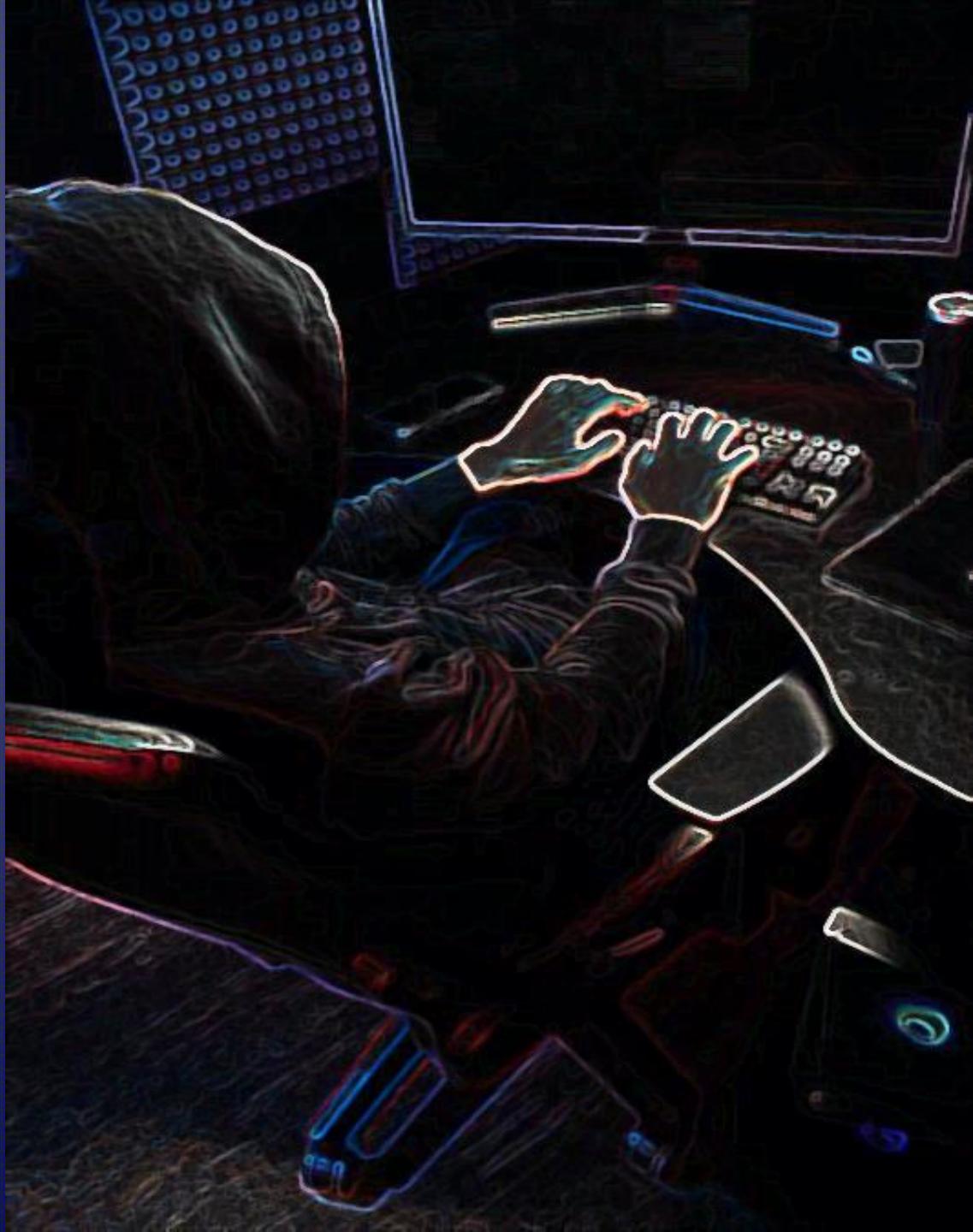
THANK YOU



github.com/BushidoUK

Twitter.com/BushidoToken

bushidotoken.net





REFERENCES

- <https://www.youtube.com/watch?v=ZDHHGZIEfsQ>
- <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>