U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Nation State Actor Cyber Threats

Ian Moore, CISSP

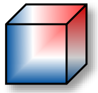
Cybersecurity State Coordinator (CSC) for Washington State

Cybersecurity Advisor (CSA) Program

Cybersecurity and Infrastructure Security Agency

Challenge - Rules of Engagement

I’ve placed several cubes, like the one below, throughout this presentation. Count all the cubes and write the total number on the back of your business card and bring it to the CISA booth to get a prize.



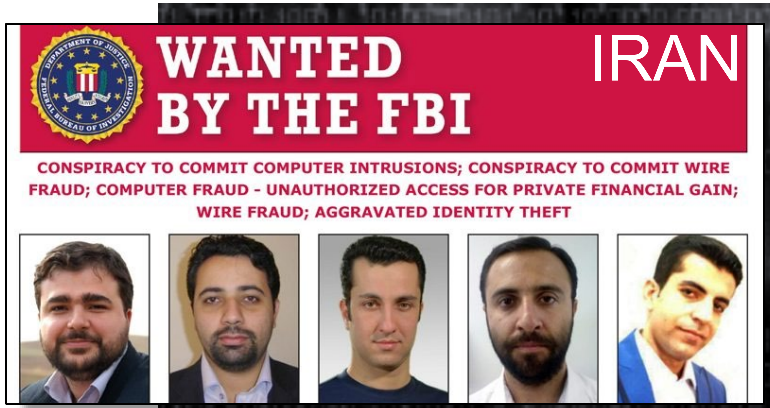
This one not counted.

- Only 1 prize per person, the first 20 get the main prize

Contents

- Who is targeting you?
- Russia - Overall Assessment
- Russia Historically
- ICS/OT Threats
- SolarWinds / Exchange / O365 Malware
- MITRE ATT@CK TTP Framework
- Detection
- Incident Response
- Destructive Malware
- Summary of Best Practices

Who is targeting you?

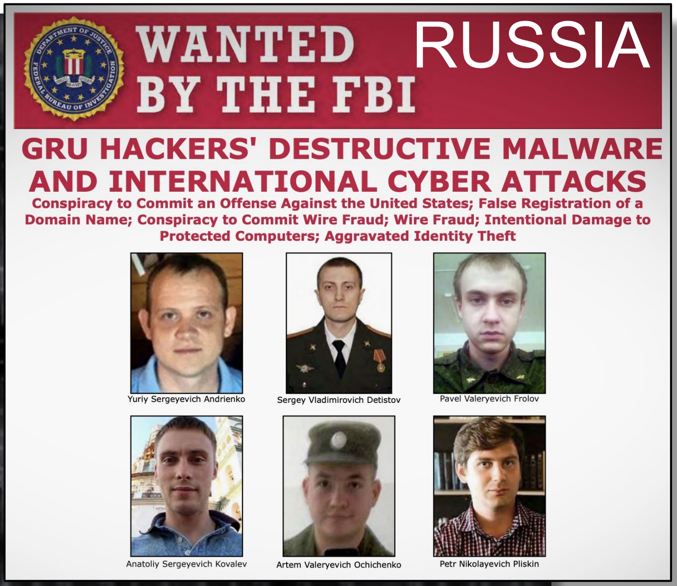


WANTED BY THE FBI

IRAN

CONSPIRACY TO COMMIT COMPUTER INTRUSIONS; CONSPIRACY TO COMMIT WIRE FRAUD; COMPUTER FRAUD - UNAUTHORIZED ACCESS FOR PRIVATE FINANCIAL GAIN; WIRE FRAUD; AGGRAVATED IDENTITY THEFT

Nation-states



WANTED BY THE FBI

RUSSIA

GRU HACKERS' DESTRUCTIVE MALWARE AND INTERNATIONAL CYBER ATTACKS

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

Yuriy Sergeyevich Andrienko

Sergey Vladimirovich Detistov

Pavel Valeryevich Frolov

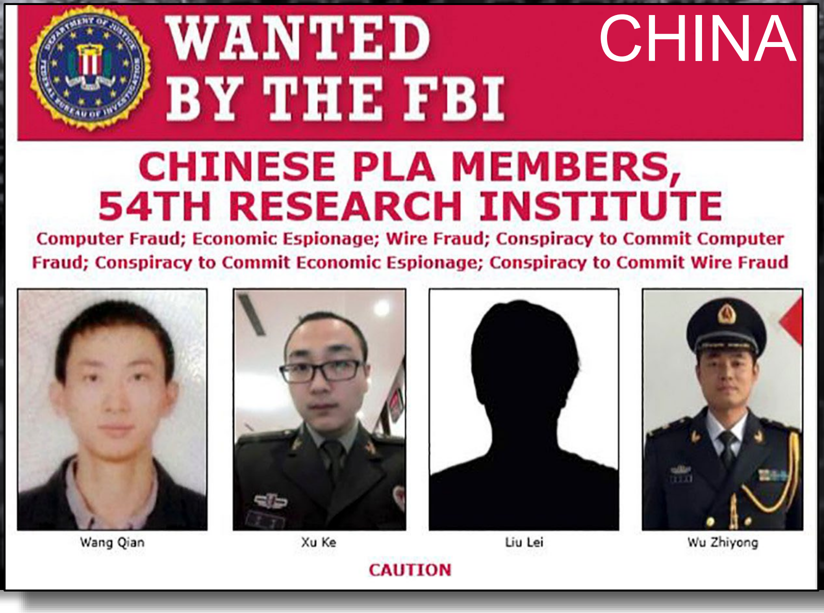
Anatoliy Sergeyevich Kovalev

Artem Valeryevich Ochichenko

Petr Nikolayevich Pliskin

Terrorists

Human Trafficking Rings



WANTED BY THE FBI

CHINA

CHINESE PLA MEMBERS, 54TH RESEARCH INSTITUTE

Computer Fraud; Economic Espionage; Wire Fraud; Conspiracy to Commit Computer Fraud; Conspiracy to Commit Economic Espionage; Conspiracy to Commit Wire Fraud

Wang Qian

Xu Ke

Liu Lei

Wu Zhiyong

CAUTION

Crime-as-a-service

Hacktivism/ Hacktivists

Russia - Overall assessment

- **"Russia continues to target critical infrastructure, including underwater cables and industrial control systems, in the United States and in allied and partner countries, as compromising such infrastructure improves—and in some cases can demonstrate—its ability to damage infrastructure during a crisis.“**
  - U.S. Office of the Director of National Intelligence 2021 Annual Threat Assessment

https://www.cisa.gov/uscert/russia

Russia Historically

Historically, Russian state-sponsored advanced persistent threat (APT) actors have used common but effective tactics—including spearphishing, brute force, and exploiting known vulnerabilities against accounts and networks with weak security—to gain initial access to target networks.

Vulnerabilities known to be exploited by Russian state-sponsored APT actors for initial access include:

- CVE-2018-13379 FortiGate VPNs
- CVE-2019-1653 Cisco router
- CVE-2019-2725 Oracle WebLogic Server
- CVE-2019-7609 Kibana
- CVE-2019-9670 Zimbra software
- CVE-2019-10149 Exim Simple Mail Transfer Protocol
- CVE-2019-11510 Pulse Secure
- CVE-2019-19781 Citrix
- CVE-2020-0688 Microsoft Exchange
- CVE-2020-4006 VMWare (note: this was a zero-day at time.)
- CVE-2020-5902 F5 Big-IP
- CVE-2020-14882 Oracle WebLogic
- CVE-2021-26855 Microsoft Exchange (Note: this vulnerability is frequently observed used in conjunction with CVE-2021-26857, CVE-2021-26858, and CVE-2021-27065)

CVE - Common Vulnerabilities and Exposures

Russian state-sponsored APT actors have also demonstrated sophisticated tradecraft and cyber capabilities by compromising **third-party infrastructure**, compromising **third-party software**, or developing and deploying custom malware.

The actors have also demonstrated the ability to **maintain persistent, undetected, long-term access** in compromised environments—including cloud environments—by using legitimate credentials.

https://www.cisa.gov/known-exploited-vulnerabilities

ICS/OT Threats

In some cases, Russian state-sponsored cyber operations against critical infrastructure organizations have specifically targeted **operational technology (OT)/industrial control systems (ICS) networks** with destructive malware.

- ICS Advisory ICS Focused Malware – Havex
  - https://us-cert.cisa.gov/ics/advisories/ICSA-14-178-01
- ICS Alert Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)
  - https://us-cert.cisa.gov/ics/advisories/ICSA-14-178-01
- ICS Alert Cyber-Attack Against Ukrainian Critical Infrastructure
  - https://us-cert.cisa.gov/ics/alerts/IR-ALERT-H-16-056-01
- Technical Alert CrashOverride Malware
  - https://us-cert.cisa.gov/ncas/alerts/TA17-163A
- CISA MAR HatMan: Safety System Targeted Malware (Update B)
  - https://us-cert.cisa.gov/ics/MAR-17-352-01-HatMan-Safety-System-Targeted-Malware-Update-B
- CISA ICS Advisory Schneider Electric Triconex Tricon (Update B)
  - https://us-cert.cisa.gov/ics/advisories/ICSA-18-107-02

SolarWinds / Exchange / O365 Malware

Just a few malware titles Russian APTs have been known to use in the past and associated with the SolarWinds and Exchange/O365 breaches/attacks

- Sunburst
- Teardrop
- Sunshuttle
- WELLMESS
- WELLMAIL
- GoldFinder
- GoldMax
- Sibot
- Open-source Red Team command and control frameworks (Sliver and Cobalt Strike)

MITRE ATT@CK Framework

Common Tactics and Techniques Employed by Russian State-Sponsored APT Actors

Tactic	Technique	Procedure
Reconnaissance [TA0043]	Active Scanning: Vulnerability Scanning [T1595.002]	Russian state-sponsored APT actors have performed large-scale scans in an attempt to find vulnerable servers.
	Phishing for Information [T1598]	Russian state-sponsored APT actors have conducted spearphishing campaigns to gain credentials of target networks.
Resource Development [TA0042]	Develop Capabilities: Malware [T1587.001]	Russian state-sponsored APT actors have developed and deployed malware, including ICS-focused destructive malware.
Initial Access [TA0001]	Exploit Public Facing Applications [T1190]	Russian state-sponsored APT actors use publicly known vulnerabilities, as well as zero-days, in internet-facing systems to gain access to networks.
	Supply Chain Compromise: Compromise Software Supply Chain [T1195.002]	Russian state-sponsored APT actors have gained initial access to victim organizations by compromising trusted third-party software. Notable incidents include M.E.Doc accounting software and SolarWinds Orion.
Execution [TA0002]	Command and Scripting Interpreter: PowerShell [T1059.003] and Windows Command Shell [T1059.003]	Russian state-sponsored APT actors have used cmd.exe to execute commands on remote machines. They have also used PowerShell to create new tasks on remote machines, identify configuration settings, exfiltrate data, and to execute other commands.
Persistence [TA0003]	Valid Accounts [T1078]	Russian state-sponsored APT actors have used credentials of existing accounts to maintain persistent, long-term access to compromised networks.
Credential Access [TA0006]	Brute Force: Password Guessing [T1110.001] and Password Spraying [T1110.003]	Russian state-sponsored APT actors have conducted brute-force password guessing and password spraying campaigns.
	OS Credential Dumping: NTDS [T1003.003]	Russian state-sponsored APT actors have exfiltrated credentials and exported copies of the Active Directory database ntds.dit.
	Steal or Forge Kerberos Tickets: Kerberoasting [T1558.003]	Russian state-sponsored APT actors have performed “Kerberoasting,” whereby they obtained the Ticket Granting Service (TGS) Tickets for Active Directory Service Principal Names (SPN) for offline cracking.
	Credentials from Password Stores [T1555]	Russian state-sponsored APT actors have used previously compromised account credentials to attempt to access Group Managed Service Account (gMSA) passwords.
	Exploitation for Credential Access [T1212]	Russian state-sponsored APT actors have exploited Windows Netlogon vulnerability CVE-2020-1472 to obtain access to Windows Active Directory servers.
	Unsecured Credentials: Private Keys [T1552.004]	Russian state-sponsored APT actors have obtained private encryption keys from the Active Directory Federation Services (ADFS) container to decrypt corresponding SAML signing certificates.
Command and Control [TA0011]	Proxy: Multi-hop Proxy [T1090.003]	Russian state-sponsored APT actors have used virtual private servers (VPSs) to route traffic to targets. The actors often use VPSs with IP addresses in the home country of the victim to hide activity among legitimate user traffic.

2021 Ransomware Trends

- **Targeting**
  - Cloud infrastructure, industrial processes, and software supply chains
  - Organizations on holidays and weekends when offices are normally closed
- **Top 3 initial infection vectors are:**
  - Phishing emails
  - Exploiting remote desktop protocol (RDP)
  - Exploiting vulnerabilities in software
- **Increasing use of ransomware-as-a-service (RaaS)** - cyber criminals employed independent services to negotiate payments, assist victims with making payments, and arbitrate payment disputes between cyber criminals.
- **Use of “triple extortion”** - (1) encrypt your data, (2) to threaten to publicly release your stolen sensitive data, and (3) then to inform your partners, shareholders, suppliers, and customers about the incident

Detection

- Implement robust log collection and retention
  - Without a centralized log collection and monitoring capability, organizations have limited ability to investigate incidents or detect the threat actor behavior
- Look for behavioral evidence or network and host-based artifacts
  - Look for suspicious **“impossible logins,”** such as logins with changing username, user agent strings, and IP address combinations or logins where IP addresses do not align to the expected user’s geographic location.
  - Look for **one IP used for multiple accounts**, excluding expected logins.
  - Look for **“impossible travel.”**
  - Look for processes and program execution command-line arguments that may indicate **credential dumping**, especially attempts to access or copy the **ntds.dit** file from a domain controller.
  - Look for **suspicious privileged account** use **after resetting passwords** or applying user account mitigations.
  - Look for **unusual activity** in typically dormant accounts.
  - Look for **unusual user agent strings**, such as strings not typically associated with normal user activity, which may indicate bot activity.

Incident Response

Organizations detecting potential APT activity in their IT or OT networks should:

- Immediately isolate affected systems
- Secure backups
  - Ensure your backup data is offline and secure
  - If possible, scan your backup data with an antivirus program to ensure it is free of malware
- Collect and review relevant logs, data, and artifacts
- Consider soliciting support from a third-party IT organization to provide subject matter expertise, ensure the actor is eradicated from the network, and avoid residual issues that could enable follow-on exploitation

Report incidents to CISA https://www.cisa.gov/uscert/report and/or the FBI via your local FBI field office http://www.fbi.gov/contact-us/field or the FBI's 24/7 CyWatch at (855) 292-3937 or CyWatch@fbi.gov.

Destructive malware targeting Ukrainian organizations

- WhisperGate (e.g., DoS:Win32/WhisperGate.A!dha)
- Stage 1: Overwrite Master Boot Record (MBR) to display a faked ransom note
- Stage 2: File corrupter malware
- Recommended Actions
  - Use IOCs
  - Review all authentication activity for remote access infrastructure
  - Enable multifactor authentication (MFA) to mitigate potentially compromised credentials and ensure that MFA is enforced for all remote connectivity
  - Enable Controlled Folder Access (CFA) in Microsoft Defender for Endpoints to prevent MBR modification

https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/

Summary of Best Practices

- IDS/IPS
- Managed Remote Access for Vendors
- Strict Access Control
  - Zero Trust
  - MFA
  - Strong Passwords
  - Least Privilege
  - Separation of Duties
- Robust Backups (Offsite, Encrypted & Tested)

- Network Segmentation
- Cyber-trained Technicians
- SIEM for log aggregation/correlation
- Managed Alerts
- Phishing Training and Awareness
- Email Filtering
- Cyber Insurance Awareness
- Incident Response Plan
- Backup Comms Plan

Conclusion

- Who is targeting you?
- Russia - Overall Assessment
- Russia Historically
- ICS/OT Threats
- SolarWinds / Exchange / O365 Malware
- MITRE ATT@CK TTP Framework
- Detection
- Incident Response
- Destructive Malware
- Summary of Best Practices

CISA Cyber Resources
https://www.cisa.gov/cyber-resource-hub

CISA Assessments and Services

Cyber Resilience Review

CRR
- 6-8 hours
- Maturity levels
- 10 Domains
- 299 Questions
- Designed for larger organizations
- Our “Grand-Daddy” Assessment

External Dependencies Management

EDM
- 4 Hours
- Supply Chain Risk Mgmt
- Relationships
- Service Resilience
- Vendor/Supplier Management

Cyber Infrastructure Survey

CIS
- 2.5–4 Hours
- 80+ Security Controls
- 5 Domains
- “CRR Light”
- Designed for small/mid-sized orgs

Cybersecurity Evaluations Tool

CSET
- Endpoint Assessment
- Downloadable
- Ransomware Readiness Assessment
- Device specific

Cyber Protective Visit

CPV
- 1 page – 1 hour
- Used to determine additional services
- For previously unknown orgs
- Basic cybersecurity questions

Region 10 Cybersecurity Contacts and Questions?

We Stop Ransomware!

Chris Callahan
Chief, Cybersecurity (CCS)
(202) 702-6706
CHRISTOPHER.CALLAHAN@cisa.dhs.gov

Theresa Masse
CSC for Oregon
503-930-5671
theresa.masse@cisa.dhs.gov

Josh Stemp
CSC for Idaho
208-761-9882
joshua.stemp@cisa.dhs.gov

Ron Watters, GSLC
Region 10 (WA, OR, ID, AK)
Cybersecurity Advisor
(206) 348-4071
Ronald.Watters@cisa.dhs.gov

Contact CISA (via the reporting portal or by phone at 1-888-282-0870) to report an intrusion or to request either technical assistance or additional resources for incident response.
CyberLiaison@cisa.dhs.gov

Mark Breunig
CSC for Alaska
907-795-5673
mark.breunig@cisa.dhs.gov

Ian Moore
CSC for Washington
(360) 594-1832
Ian.Moore@cisa.dhs.gov

For inquiries or further information,
contact cyberadvisor@cisa.dhs.gov