Major Cyber Organizations of the Russian Intelligence Services

May 19, 2022
Agenda

- Russian Intelligence Services’ Structure
- Russian Intelligence Services’ Mandates
- Turla
- APT29
- APT28
- Sandworm
- Conclusion
- Questions

Slides Key:

- **Non-Technical**: Managerial, strategic and high-level (general audience)
- **Technical**: Tactical / IOCs; requiring in-depth knowledge (sysadmins, IRT)
Russian Intelligence Services’ Structure
Russian Intelligence Services’ Mandates

The Federal Security Service (FSB) - FBI equivalent
Collect on domestic intelligence and security, plus foreign intelligence from Russia’s Near Abroad.

The Foreign Intelligence Service (SVR) - CIA equivalent
Collect foreign intelligence from military, strategic, economic, scientific, and technological targets; conduct active measures.

The Main Intelligence Directorate of the General Staff of the Armed Forces (GRU) - DIA equivalent
Collect foreign intelligence focusing on military issues; also conducts information operations and destructive cyber attacks.

Source: Mandiant

Source: European Council on Foreign Relations
Disclaimer

Organizations track cyber threat actors using varying methodologies.

In this presentation we have:
- Used Mandiant’s designation to refer to the actor.
- Used CrowdStrike’s visual depiction of the actor, known as “bears”.
- Gone back to the earliest suspected activity we could find.

Source: Cyb3rops
Turla

- **Attribution**: Russia’s FSB
- **Earliest suspected activity**: 2004
- **AKA**: Venomous Bear (CrowdStrike), CTG-8875 (SCWX CTU), ITG12 (IBM), KRYPTON (Microsoft), Waterbug (Symantec), Iron Hunter (Secureworks)
- **Targeted Industries**: Academic, Embassies, Energy, Government, Military, Telecommunications, Research and Pharmaceutical Companies

Source: CrowdStrike
Turla: Noteworthy Attacks

• U.S. Central Command (2008)
• Former Soviet Union Prime Minister’s office (2012)
• G20 attendees (2017)
  ▪ Embedded a malware dropper in a meeting invite
  ▪ Dropper installed a JavaScript decryptor, which in turn installed the KopiLuwak backdoor
• Germany’s government computer network (2018)
Turla Malware & Tactics, Techniques, and Procedures (TTPs)

- **Known Associated Malware:**
  - Carbon-DLL, ComRAT, Mosquito, Nautilus, Neuron, PoisonFrog, PyFlash, Skipper, Snake, Tavdig
  - LightNeuron
    - Sophisticated backdoor that has targeted Microsoft Exchange servers since 2014

- **Tactics, Techniques, and Procedures (TTPs):**
  - Largely focused on former Eastern Bloc countries
  - Uses novel and sophisticated techniques to maintain OPSEC
  - Espionage-focused actor in search of diplomatic intelligence
  - Distinct command and control network probably supported by SIGINT assets
  - Started using a second, simple, limited-functionality backdoor to maintain persistence if primary backdoor was discovered
APT29

- **Attribution:** Russia’s SVR
- **Earliest suspected activity:** 2008
- **AKA:** Cozy Bear (CrowdStrike), The Dukes (F-Secure), YTTRIUM (Microsoft), Iron Hemlock (Secureworks)
- **Targeted Industries:** Academic, Energy, Financial, Government, Healthcare, Media, Pharmaceutical, Technology, Think Tanks

Source: CrowdStrike
APT29: Noteworthy Attacks

• Pentagon (2015)
• COVID-19 vaccine developers (2020)
• SolarWinds Orion attack (2020)
  ▪ Used a trojanized version of SolarWind’s Orion software updates to distribute SUNBURST backdoor
  ▪ Leveraged lateral movement and stole data
  ▪ 18,000 affected — including a U.S. hospital
APT 29 Malware & Tactics, Techniques, and Procedures (TTPs)

- Known Associated Malware:
  - FatDuke
    - Flagship backdoor
    - Generally dropped by the MiniDuke backdoor but also using lateral movement such as PsExec

- Tactics, Techniques, and Procedures (TTPs):
  - Primarily targets European and NATO countries
  - Leverages large-scale spear phishing campaigns
  - Especially persistent and focused on specific targets
  - Prefers stealthy, long-term operations
  - Often reuses tools and techniques from previous attacks
  - Steals information, but doesn’t leak it like APT28
APT28

- **Attribution:** Russia’s GRU, 85th Main Special Service Center, Military Unit 26165
- **Earliest suspected activity:** 2004
- **AKA:** Fancy Bear (Crowdstrike), Group 74 (Talos), PawnStorm (Trend Micro), Sednit (ESET), Snakemackerel (iDefense), Sofacy (Palo Alto), STRONTIUM (Microsoft), TG-4127 (SCWX CTU), Tsar Team (iSight), Iron Twilight (Secureworks)
- **Targeted Industries:** Aerospace, Defense, Energy, Government, Healthcare, Military, Media, Dissidents

Source: CrowdStrike
APT28: Noteworthy Attacks

• World Anti-Doping Agency (2016)
  ▪ Posed as hacktivists
  ▪ Stole and manipulated the data in their systems
  ▪ Act of revenge

• U.S. Democratic National Committee and the Clinton Campaign (2016)
  ▪ Stole a great amount of data, including 19,252 emails from DNC staffers and members of Clinton’s campaign

• German and French Elections (2016-2017)

• International Olympic Committee (2018)
APT28 Malware & Tactics, Techniques, and Procedures (TTPs)

• Known Associated Malware:
  ▪ DEALERSCHOICE, Downdelph, EVILTOSS, HIDEDRV, LoJack, PowerShell Empire, Scaramouche, SCONATO, Sedkit Exploit Kit, SHARPFRONT, Sofacy downloader, X-Agent, X-Tunnel, Zebrocy
  ▪ SEDUPLoader
    • Simple tool used to facilitate download and persistence of next-stage tool
    • Collects system information and metadata, probably to tell sandbox environments apart from real targets

• Tactics, Techniques, and Procedures (TTPs)
  ▪ Primarily focuses on NATO countries
  ▪ Uses password spraying techniques
  ▪ Uses malware unique to APT28 and leverages proprietary tools and droppers
  ▪ Employs phishing and credential harvesting
    • Targets conventional computers and mobile devices
  ▪ Steals and leaks information for publicity to further Russia’s political interests
  ▪ Conducts “noisy” cyber attacks
**Sandworm**

- **Attribution:** Russia’s GRU, Main Center for Special Technologies, Unit 74455
- **Earliest suspected activity:** 2007
- **AKA:** Voodoo Bear (CrowdStrike), CTG-7263 (SCWX CTU), ELECTRUM (Dragos), Hades/OlympicDestroyer (Kaspersky), IRIDIUM (Microsoft), IRIDUM (Microsoft), Qudedagh (F-Secure), Sandworm Team (Trend Micro), Telebots (ESET), Iron Viking (Secureworks)
- **Targeted Industries:** Energy, Government

*Source: CrowdStrike*
Sandworm: Noteworthy Attacks

• Ukrainian Government and Critical Infrastructure (2015-2016, 2022)
• Georgian websites prior to Russian invasion (2008)
  ▪ Used DDoS attacks
  ▪ 54 targets including government, financial, and media outlets
• NotPetya attacks (2017)
  ▪ Hijacked Ukrainian accounting software MeDoc (the TurboTax of Ukraine)
  ▪ Corrupted the update so that if you had a copy of MeDoc, you had a copy of NotPetya
  ▪ Shut down a pharmaceutical manufacturer in the U.S.
  ▪ Affected the medical record systems of dozens of U.S. hospitals.
Sandworm Malware & Tactics, Techniques, and Procedures (TTPs)

• Known Associated Malware:
  - BadRabbit, BlackEnergy, GCat, GreyEnergy, KillDisk, NotPetya, PSCrypt, TeleBot, TeleDoor, xData
  - Industroyer
    • Speaks several industrial communication protocols that are used worldwide in critical infrastructure systems
    • Uses a wiper module to make systems unbootable; erases system crucial registry keys and overwrites files

• Tactics, Techniques, and Procedures (TTPs)
  - Particular focus on Ukraine
  - Targets ICS and computer systems for destructive purposes, such as shutting down power plants or deleting data
  - Most destructive of the “Bears” and seemingly not concerned with 2nd/3rd order effects of attacks (i.e., NotPetya)
Mitigations

• Update software, including operating systems, applications, and firmware, on IT network assets
• Reviewing the CVEs for all Public Facing Systems – CISA regularly updates and maintains a full list of CVEs that are known to be exploited: [CISA: Known Exploited Vulnerabilities Catalog](CISA: Known Exploited Vulnerabilities Catalog)
• Enforce MFA to the greatest extent possible and require accounts with password logins, including service accounts, to have strong passwords
• If you use RDP and/or other potentially risky services, secure and monitor them closely
• Provide end-user awareness and training to help prevent successful targeted social engineering and spear phishing campaigns
• As part of a longer-term effort, implement network segmentation to separate network segments based on role and functionality
• HHS 405(d) program provides the Healthcare and Public Health (HPH) sector with useful, impactful, and vetted resources, products, videos, and tools that help raise awareness and provide cybersecurity practices, which drive behavioral change and move toward consistency in mitigating the most relevant cybersecurity threats to the sector. They offer advice for small, medium, and large healthcare organizations: [405(d) Health Industry Cybersecurity Practices (HICP)](405(d) Health Industry Cybersecurity Practices (HICP))
• For more information on preparing for cyber incidents, identity and access management tips, protective controls and architecture, and vulnerability and configuration management, see the CISA joint cybersecurity advisory [Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure](Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure)
Conclusion

Source: Euro Maidan Press
References I

References II


References III

- “Mitre ATT&CK Groups,” Mitre ATT&CK. https://attack.mitre.org/groups/
Questions
FAQs

Upcoming Briefing
• June 2, 2022 – The Return of Emotet

Product Evaluations
Recipients of this and other Healthcare Sector Cybersecurity Coordination Center (HC3) Threat Intelligence products are highly encouraged to provide feedback. To provide feedback, please complete the HC3 Customer Feedback Survey.

Requests for Information
Need information on a specific cybersecurity topic? Send your request for information (RFI) to HC3@HHS.GOV.

Disclaimer
These recommendations are advisory and are not to be considered as federal directives or standards. Representatives should review and apply the guidance based on their own requirements and discretion. The HHS does not endorse any specific person, entity, product, service, or enterprise.
About HC3

The Health Sector Cybersecurity Coordination Center (HC3) works with private and public sector partners to improve cybersecurity throughout the Healthcare and Public Health (HPH) Sector. HC3 was established in response to the Cybersecurity Information Sharing Act of 2015, a federal law mandated to improve cybersecurity in the U.S. through enhanced sharing of information about cybersecurity threats.

What We Offer

| Sector and Victim Notifications | Direct communications to victims or potential victims of compromises, vulnerable equipment, or PII/PHI theft, as well as general notifications to the HPH about current impacting threats via the HHS OIG. |
| Alerts and Analyst Notes | Documents that provide in-depth information on a cybersecurity topic to increase comprehensive situational awareness and provide risk recommendations to a wide audience. |
| Threat Briefings | Presentations that provide actionable information on health sector cybersecurity threats and mitigations. Analysts present current cybersecurity topics, engage in discussions with participants on current threats, and highlight best practices and mitigation tactics. |
Contacts

HHS.GOV/HC3

HC3@HHS.GOV