Recent Activity of Russian Threat Groups

Luke McNamara
Principal Analyst, FireEye Intelligence
SOSSEC Membership is Required for COBRA Awards

Benefits of Joining the SOSSEC Consortium

✓ Opportunity to perform work under seven (7) OTAs for the Air Force, Army and National Geospatial-Intelligence Agency
✓ Opportunity to build members’ business base by applying their technologies/expertise to meeting urgent DoD requirements
✓ Simple, streamlined process to compete for DoD work
✓ Average 60 days from requirements definition to award
✓ Flexible treatment of intellectual property
✓ OTA access to any DoD user with approval of OTA customer

Go to [www.sossecinc.com](http://www.sossecinc.com) and click on the JOIN NOW Tab to access the membership application. The process is simple and rapid. There is no joining fee, and the membership fee is $500 per year. Membership is open to Industry (traditional, nontraditional, small business), not for profit and academic institutions that share the values of the SOSSEC Consortium.
Comparison of 15 Vendors Against 10 Criteria

- **FireEye is THE ONLY leader among the group**

- **“Leads the pack with collection capabilities”**
  - We “marry digital forensics, human intelligence (HUMINT), and a global sensor network” – synching adversary, victim, and campaign intel with product telemetry
  - Global real-world incident response provides up-to-date data

- **“Best fit for companies desiring a breadth of outcomes from a single vendor”** – we provide…
  - Threat indicator **feeds** with high-efficacy alerts
  - **Services** that growing overall security intelligence capabilities
  - **Finished threat intelligence** leaders can use to make proactive and informed decisions

---

*The Forrester New Wave™: External Threat Intelligence Services, Q3 2018* by Josh Zelonis, September 7, 2018

The Forrester New Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester New Wave™ is a graphical representation of Forrester's call on a market. Forrester does not endorse any vendor, product, or service depicted in the Forrester New Wave™. Information is based on best available resources.
No One Knows More About The Adversary Than FireEye

**Machine Intelligence**
- 16m+ email, endpoint, network sensors globally
- Tens of millions of MVX detonations per hour

**Victim Intelligence**
- 13+ years of investigative expertise
- 200+ of the Fortune 500
- 26 countries with consultants

**Adversary Intelligence**
- 22 countries
- 30+ languages natively
- 170+ analysts and researchers

**Campaign Intelligence**
- 7 Security Operations Centers
- 99m+ events ingested
- 21m+ alerts validated by Intel
- 33,700+ incidents dispositioned

**Actionable Intelligence**
- Multi-faceted, forward looking, validated, highly contextual analysis

**Who/What?**
- Actors
- Groups
- Government Sponsors

**Why/When?**
- Motivation
- Intent
- Capabilities

**How?**
- TTPs
- Methods
- Playbooks
M-Trends 2020 – Key Takeaways

• the media/entertainment industry is most targeted, jumping to first place from fifth just one year ago

• there was a 28 percent decrease in the global median time from compromise to discovery or dwell time – a trend our experts attribute to organizations improving their detection programs, as well as changes in attacker behaviors

• disruptive attacks such as ransomware and cryptocurrency miners increased

• of the malware families that were seen in 2019, 41 percent had never been seen before

• 70 percent of the malware samples identified belonged to one of the five most frequently seen families, demonstrating that malware authors are innovating and cyber criminals are outsourcing tasks to monetize operations faster

• for the first time in four years, external notifications – when an outside entity informs an organization that it has been compromised – exceeded internal detections

• the majority of attacks were likely motivated by direct financial gain, with the successful monetization of ransomware driving an increase in these cases; second most common was data theft
Agenda

- FireEye’s perspective
- Russian APT groups
  - APT28
  - APT29
  - Sandworm Team
  - Turla
  - TEMP.Armageddon
  - TEMP.Isotope
  - TEMP.Veles
- Recent information operations activity
Our perspective

**Adversarial intelligence:** What healthcare data is being sold in the underground?

**Victim Intelligence:** What data are actors targeting? What additional tools are they using?

**Global sensor network:** How broad is this spear-phishing campaign?
Russian APT Groups
APT Groups

- APT28
- APT29
- Sandworm Team
- Turla
- TEMP.Armageddon
- TEMP.Isotope
- TEMP.Veles
Key Themes

- European MFAs continue to be a heavy area of focus for multiple Russian threat groups.
- Similar to other nation state adversaries, usage of open source malware and frameworks has increased (likely in part to hamper attribution).
- Suspected continued blend of cyber espionage and information operations.
- Continued focus on understanding potential operational connections between some APT groups believed to be part of the same organization.
- Continued examination of when destructive capabilities are utilized.
Key TTPs

- Continued use of phishing campaigns with malicious attachments or links: Russian espionage groups continue to widely leverage phishing campaigns as a means of harvesting credentials, distributing malware, and other means to facilitate initial compromise.

- Decreased observed use of zero-day vulnerabilities: Previously, we observed that APT28 deployed the highest number of zero day exploits compared to other actors from 2012 to 2017.
  - In the last two years, APT28 and other Russian espionage actors appear to have primarily leveraged known vulnerabilities for which patches were recently made available but potentially not yet applied.

- Continued use of strategic web compromise: Multiple Russian espionage groups, including TEMP.Isotope, Sandworm Team, and likely Turla, have been suspected to have used strategic web compromises (watering hole attacks).
Q4 2019 Activity

Russia-nexus APT activity was dominated by TEMP.Armageddon and Turla Team actors that carried out aggressive campaigns targeting European and Western entities, especially in Ukraine.
APT28 (Tsar Team, Fancy Bear)

- Most prolific group that we have observed over the last couple years (tracked since 2007).

- The group primarily focuses on governments, diplomatic institutions, DIB, NATO, EU, and previous member states of the former Soviet Union. Secondary targeting of organizations in media, entertainment, and publishing; international sporting organizations; hospitality; manufacturing and construction; and technical and research verticals.

- Connection to multiple hacktivist fronts (CyberCaliphate, AnPoland, CyberBerkut, etc.)

- Mixture of open source (PowerShell Empire) and custom (GAMEFISH) malware.

- Spoofing of domains used for credential collection and phishing common.
APT29 (Office Monkeys, Cozy Bear, the Dukes)

- APT29 boasts sophisticated capabilities, to include a range of custom developed tools, extensive command and control (C&C) infrastructure that includes compromised and satellite infrastructure (via apparent service providers), and savvy operational know-how.

- Notable activity: 2016 DNC compromise

- In late 2018 our devices detected spearphishing activity across multiple industries using a legitimate document taken from the U.S. Department of State's website to deploy CobaltStrike BEACON, a publicly available backdoor. The TTPs, targeting, and coding fragments contain significant overlap with previous APT29 campaigns.

- It is still unclear whether APT29 has reorganized or disbanded and dispersed its tools and operators into other portions of the Russian government, taken a hiatus to develop new tools, or focused only on highly plausibly deniable or hard to detect campaigns.
Sandworm Team


- Potential utilization of similar resources with APT28 for domain registration

- 2019 observance of FAIRROOT (macro delivering obfuscated .NET application deploying PowerShell Empire) and potential targeting of mobile developers

- Lure content suggests that these documents are geared toward Russian, Ukrainian, and Urdu speakers, potentially located in Azerbaijan and Pakistan
Turla

- Stealthy, longstanding group with historical ties to Agent.BTZ malware
- Despite the UK’s NCSC public disclosures of Turla’s use of DARKNEURON in conjunction with other new malware, (NAUTILUS, WEATHERMAN, BIRDPEN, FAÇADE) Turla continues to use DARKNEURON along with a wide range of other proprietary and publicly available malware. However, there have been no major changes to DARKNEURON since that time.
  - In one case, Iranian APT infrastructure (APT34) was reportedly used to deploy an implant, and later, Turla infrastructure accessed the same implant, suggesting that Turla likely had some access to controller software.
- In early February 2020, FireEye Threat Intelligence uncovered a new DARKNEURON campaign likely targeting Georgian government entities. Based on targeting and historic use of DARKNEURON, we assess with moderate to high confidence that Turla is continuing to use this malware despite public disclosures.
- Currently investigating similar campaigns in Europe
TEMP.Armageddon (Gameredon)

- Active and carrying out operations against Ukraine since at least 2013. Historical reporting indicates that TEMP.Armageddon has a deep and singular interest in Ukrainian political, military, and security issues, particularly relating to the ongoing conflict in Eastern Ukraine.

- Further, from mid-2013 through at least March 2015, TEMP.Armageddon relied heavily on off-the-shelf tools to conduct operations. However, more recent activity has used custom-built Windows batch script, suggesting that the group is becoming more sophisticated (ARMEDCLOUD malware).

- Particular focus on military/security issues (example: in August 2019 two lure documents featuring themes related to U.S.-Ukrainian military and diplomatic relations were delivered to what are likely Ukrainian government and defense organizations.)
In September 2019, FireEye devices detected and blocked a TEMP.Armageddon spear-phishing campaign targeting Ukraine, as well as government and military organizations in Eastern Europe with ARMEDCLOUD malware and a variety of changes in tactics, techniques, and procedures (TTPs).

Lures and targets lead us to assess with high confidence that the overall objective of the campaign is strategic and military in nature, with perhaps an additional focus on naval activity in the Black Sea (historic targeting around Sea Breeze exercises).

One piece of malware potentially targeted Ukrainian security or police services based on lure content and submitter data. Lure content included illegal gambling in Ukraine’s Kherson Oblast region. Notably, related activity from May also referenced this region, which is strategically important to Russia given its geolocation to Crimea and access to the Black Sea.
TEMP.Isotope

- Since 2017, we have tracked an activity set that has primarily targeted ICS of critical infrastructure as TEMP.Isotope (overlap with Dragonfly 2.0)

- Suspected of targeting critical infrastructure in the US, Turkey, Ireland, and elsewhere.

- Notable usage of Server Message Block (SMB) callouts.

- Linkages to campaign targeting the Ukrainian presidential election (election related entity and media organization) using RUNOFF and TURNOUT malware
TEMP.Veles (XENOTIME)

- In 2017, FireEye Mandiant responded to an incident at a critical infrastructure organization where the threat actor TEMP.Veles deployed the TRITON attack framework designed to manipulate safety instrumented systems.

- FireEye Intelligence assesses with high confidence that intrusion activity that led to deployment of TRITON was supported by the Central Scientific Research Institute of Chemistry and Mechanics (CNIIHM), a Russian Government-owned technical research institution located in Moscow.
Russian Information Operations
Russian IO in 2019:

- **False personas**: We continue to see what we assess are false personas created to promote leaks and narratives in line with Russian strategic interests.

- **Narrative centric campaigns**: We have also observed narrative-centric campaigns that use an array of fabricated social media accounts, news sites, blog posts, and appropriated real identities.

- **Increased piggybacking**: Russian influence campaigns during the past year appear to have increasingly used existing political narratives.

- **Increased obfuscation efforts**: FireEye Threat Intelligence has noted that new accounts linked to the Internet Research Agency (IRA) appear to establish increasingly sophisticated profiles that are more likely to avoid platform detection.
Indications Sandworm and APT28 Involved in Ukrainian- and Lithuanian-Focused Influence Operations in 2018 and Early 2019

- The first operation was conducted in January 2018 with a compromise of the Ukrainian aircraft manufacturer Antonov’s website and the publication of a fabricated letter written as if by Antonov’s management with a narrative critical of the Ukrainian government.

- The second operation was conducted in April 2019, with the posting of a false article to the website of the Lithuanian news outlet "Kas Vyksta Kaune," stating that the Lithuanian Minister of Defense was suspected of corruption.

- IPs from email senders in both these incidents used to contact media in an effort to generate attention to this activity aligned with domain registration and SSL certificate patterns to known APT28 and Sandworm Team infrastructure procurement behavior for potential credential harvesting efforts.
Suspected Russian Information Operations

- **July 2019**, we reported on an operation leveraging a suspected forged letter, purportedly from U.S. Senator Ben Cardin addressed to Senator Robert Menendez, as source material to promote a narrative that the U.S. was seeking to work with the Russian opposition to overthrow the Putin regime.

- Ukrainian and Lithuanian presidential elections from **March through May 2019**, we observed two related operations. Those operations leveraged what we assessed with low confidence to be fabricated Facebook private messages between Ukrainian and Pittsburgh, PA, Jewish community leaders, and between a Lithuanian presidential candidate and a former Ambassador of Georgia to Lithuania.

- **August 2019**, we reported an operation that began on July 29, 2019, that promoted disinformation surrounding recent anti-Russia protests in Tbilisi, Georgia, including a suspected fabricated Security Service of Ukraine (SBU) memorandum as source material to promote a narrative alleging Ukrainian and U.S. support in the Georgian protests.

- **August 2019**, we reported an operation that leveraged suspected fabricated WhatsApp chats between an employee of the U.S. Embassy in Kazakhstan and an unknown party, which were used as source material to promote the narrative that the U.S. Government is planning to organize a coup in Kazakhstan.
Fabricated Letter Purportedly Written by NATO StratCom Director

- On Nov. 21, 2019, Jānis Sārts, director at the North Atlantic Treaty Organization (NATO) Strategic Communications Centre of Excellence, tweeted that two fabricated letters, presented as having been authored by Sārts, had been posted online. Sārts confirmed that the letters were forgeries.

- FireEye Threat Intelligence assesses with high confidence that the fabricated letters comprise part of the broader, suspected Russian campaign that we have reported on in recent months leveraging forged government correspondence amplified via pseudo-news articles posted on online forums and blogs.

  - E.g., On Nov. 20, 2019, accounts used to disseminate the fabricated letters on Reddit and Homment, "saisioEU," and "saisio," respectively, were created. Both accounts posted pseudo-news articles to their respective platforms referencing the letters on that same day.
What to Watch For

- TEMP.Armageddon and Turla activity will be interesting to watch, especially with the former potentially expanding geographic targeting outside of Ukraine.
- Sandworm (always)
- Utilization of destructive capabilities (where and when?)
- Nexus of cyber espionage and information operations
- European election activity?
- Tokyo Olympics?
Questions