Advanced Persistent Threat Groups

Who's who of cyber threat actors

FireEye pays special attention to advanced persistent threats (APT) groups that receive direction and support from an established nation state.

Like other attackers, APT groups try to steal data, disrupt operations or destroy infrastructure. Unlike most cyber criminals, APT attackers pursue their objectives over months or years. They adapt to cyber defenses and frequently retarget the same victim.

Just because you have APT-linked malware variants in your system doesn't mean that you're an APT target. But your security team should be aware of this list of the most active APT groups and take extra precautions when they detect malware linked to previous APT attacks.

READ THE LATEST REPORT >

WEBINAR

A 360-Degree View of the Latest APT Groups

REGISTER FOR THE WEBINAR >

Suspected Attribution

Iran | China | North Korea | Russia | Vietnam | Undisclosed

SUSPECTED ATTRIBUTION: IRAN

APT39

Suspected attribution: Iran

Target sectors: While APT39's targeting scope is global, its activities are concentrated in the Middle East. APT39 has prioritized the telecommunications sector, with additional targeting of the travel industry and IT firms that support it and the high-tech industry.

Overview: The group's focus on the telecommunications and travel industries suggests intent to perform monitoring, tracking, or surveillance operations against specific individuals, collect proprietary or customer data for commercial or operational purposes that serve strategic requirements related to national priorities, or create additional accesses and vectors to facilitate future campaigns. Government entities targeting suggests a potential secondary intent to collect geopolitical data that may benefit nation-state decision making.

Associated malware: The group primarily leverages the SEAWEED and CACHEMONEY backdoors along with a specific variant of the POWBAT backdoor.

Attack vectors: For initial compromise FireEye Intelligence has observed APT39 leverage spearphishing with malicious attachments and/or hyperlinks typically resulting in a POWBAT infection. In some cases previously compromised email accounts have also been leveraged, likely to abuse inherent trusts and increase the chances of a successful attack. APT39 frequently registers and leverages domains that masquerade as legitimate web services and organizations that are relevant to the intended target. Furthermore, this group has routinely identified and exploited vulnerable web servers of targeted organizations to install web shells, such as ANTAK and ASPXSPY, and used stolen legitimate credentials to compromise externally facing Outlook Web Access (OWA) resources. We have not observed APT39 exploit vulnerabilities.

Back to top ▵

Additional resources

Blog – APT39: An Iranian Cyber Espionage Group Focused on Personal Information

---

APT34

Suspected attribution: Iran

Target sectors: This threat group has conducted broad targeting across a variety of industries, including financial, government, energy, chemical, and telecommunications, and has largely focused its operations within the Middle East

Overview: We believe APT34 is involved in a long-term cyber espionage operation largely focused on reconnaissance efforts to benefit Iranian nation-state interests and has been operational since at least 2014. We assess that APT34 works on behalf of the Iranian government based on infrastructure details that contain references to Iran, use of Iranian infrastructure, and targeting that aligns with nation-state interests.

Associated malware: POWBAT, POWRUNER, BONDUPDATER

Attack vectors: In its latest campaign, APT34 leveraged the recent Microsoft Office vulnerability CVE-2017-11882 to deploy POWRUNER and BONDUPDATER.

Back to top ▵

Additional resources

Blog – New Targeted Attack in the Middle East by APT34, a Suspected Iranian Threat Group, Using CVE-2017-11882 Exploit

---

APT33

Suspected attribution: Iran

Target sectors: Aerospace, energy

Overview: APT33 has targeted organizations, spanning multiple industries, headquartered in the U.S., Saudi Arabia and South Korea. APT33 has shown particular interest in organizations in the aviation sector involved in both military and commercial capacities, as well as organizations in the energy sector with ties to petrochemical production.

Associated malware: SHAPESHIFT, DROPSHOT, TURNEDUP, NANOCORE, NETWIRE, ALFA Shell

Attack vectors: APT33 sent spear-phishing emails to employees whose jobs related to the aviation industry. These emails included recruitment themed lures and contained links to malicious HTML application (.hta) files. The .hta files contained job descriptions and links to legitimate job postings on popular employment websites that would be relevant to the targeted individuals.

Back to top ▵

Additional resources

Blog – APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware

Webinar – Insights into Iranian Cyber Espionage Group

SUSPECTED ATTRIBUTION: CHINA

APT41

Suspected attribution: China

Target sectors: APT41 has directly targeted organizations in at least 14 countries dating back to as early as 2012. The group's espionage campaigns have targeted healthcare, telecoms, and the high-tech sector, and have historically included stealing intellectual property. Their cyber crime intrusions are most apparent among video game industry targeting, including the manipulation of virtual currencies, and attempted deployment of ransomware. APT41operations against higher education, travel services, and news/media firms provide some indication that the group also tracks individuals and conducts surveillance.

Overview: APT41 is a prolific cyber threat group that carries out Chinese state-sponsored espionage activity in addition to financially motivated activity potentially outside of state control.

Associated malware: APT41 has been observed using at least 46 different code families and tools.

Attack vectors: APT41 often relies on spear-phishing emails with attachments such as compiled HTML (.chm) files to initially compromise their victims. Once in a victim organization, APT41 can leverage more sophisticated TTPs and deploy additional malware. For example, in a campaign running almost a year, APT41 compromised hundreds of systems and used close to 150 unique pieces of malware including backdoors, credential stealers, keyloggers, and rootkits. APT41 has also deployed rootkits and Master Boot Record (MBR) bootkits on a limited basis to hide their malware and maintain persistence on select victim systems.

Back to top ▵

Additional resources

Report – APT41: A Dual Espionage and Cyber Crime Operation

Blog – APT41, A Dual Espionage and Cyber Crime Threat

Webinar – Double Dragon: APT41, a Dual Espionage and Cyber Crime Operation

---

APT40

Suspected attribution: China

Target sectors: APT40 is a Chinese cyber espionage group that typically targets countries strategically important to the Belt and Road Initiative. Although the group targets global organizations — especially those with a focus on engineering and defense — it also historically conducted campaigns against regional entities in areas such as Southeast Asia. Since at least January 2013, the group has conducted campaigns against a range of verticals including maritime targets, defense, aviation, chemicals, research/education, government, and technology organizations.

Overview: FireEye Intelligence believes that APT40's operations are a cyber counterpart to China's efforts to modernize its naval capabilities; this is also manifested in targeting wide-scale research projects at universities and obtaining designs for marine equipment and vehicles. The group's operations tend to target government-sponsored projects and take large amounts of information specific to such projects, including proposals, meetings, financial data, shipping information, plans and drawings, and raw data.

Associated malware: APT40 has been observed using at least 51 different code families. Of these, 37 are non-public. At least seven of these non-public tools (BADSIGN, FIELDGOAL, FINDLOCK, PHOTO, SCANBOX, SOGU, and WIDETONE) are shared with other suspected China-nexus operators.

Attack vectors: APT40 typically poses as a prominent individual who is probably of interest to a target to send spear-phishing emails. This includes pretending to be a journalist, an individual from a trade publication, or someone from a relevant military organization or non-governmental organization (NGO). In some instances, the group has leveraged previously compromised email addresses to send spear-phishing emails.

Back to top ▵

Additional resources

Blog – APT40: Examining a China-Nexus Espionage Actor

APT30

Suspected attribution: China

Target sectors: Members of the Association of Southeast Asian Nations (ASEAN)

Overview: APT30 is noted not only for sustained activity over a long period of time but also for successfully modifying and adapting source code to maintain the same tools, tactics and infrastructure since at least 2005. Evidence shows that the group prioritizes targets, most likely works in shifts in a collaborative environment and builds malware from a coherent development plan. The group has had the capability to infect air-gapped networks since 2005.

Associated malware: SHIPSHAPE, SPACESHIP, FLASHFLOOD

Attack vectors: APT30 uses a suite of tools that includes downloaders, backdoors, a central controller and several components designed to infect removable drives and cross air-gapped networks to steal data. APT30 frequently registers its own DNS domains for malware CnC activities.

Back to top ▵

Additional resources

Report – APT30 and the Mechanics of a Long-Running Cyber Espionage Operation: How a Cyber Threat Group Exploited Goverments and Commercial Entities across Southeast Asia and India for over a Decade

Blog – APT30 and Lessons for ASEAN

APT19

Also known as: Codoso Team

Suspected attribution: China

Target sectors: Legal and investment

Overview: A group likely composed of freelancers, with some degree of sponsorship by the Chinese government.

Associated malware: BEACON, COBALTSTRIKE

Attack vectors: In 2017, APT19 used three different techniques to attempt to compromise targets. In early May, the phishing lures leveraged RTF attachments that exploited the Microsoft Windows vulnerability described in CVE 2017-0199. Toward the end of May, APT19 switched to using macro-enabled Microsoft Excel (XLSM) documents. In the most recent versions, APT19 added an application whitelisting bypass to the XLSM documents. At least one observed phishing lure delivered a Cobalt Strike payload.

Back to top ▵

APT18

Also known as: Wekby

Suspected attribution: China

Target sectors: Aerospace and Defense, Construction and Engineering, Education, Health and Biotechnology, High Tech, Telecommunications, Transportation

Overview: Very little has been released publicly about this group.

Associated malware: Gh0st RAT

Attack vectors: Frequently developed or adapted zero-day exploits for operations, which were likely planned in advance. Used data from Hacking Team leak, which demonstrated how the group can shift resources (i.e. selecting targets, preparing infrastructure, crafting messages, updating tools) to take advantage of unexpected opportunities like newly exposed exploits.

Back to top ▵

Additional resources

Blog – Demonstrating Hustle, Chinese APT Groups Quickly Use Zero-Day Vulnerability (CVE-2015-5119) Following Hacking Team Leak

Webinar – State of the Hack: Spotlight on Healthcare

APT17

Also known as: Tailgator Team, Deputy Dog

Suspected attribution: China

Target sectors: U.S. government, and international law firms and information technology companies

Overview: Conducts network intrusion against targeted organizations.

Associated malware: BLACKCOFFEE

Attack vectors: The threat group took advantage of the ability to create profiles and post in forums to embed encoded CnC for use with a variant of the malware it used. This technique can make it difficult for network security professionals to determine the true location of the CnC, and allow the CnC infrastructure to remain active for a longer period.

Back to top ▵

Additional resources

Report – Hiding in Plain Sight: FireEye and Microsoft Expose Obfuscation Tactic

APT16

Suspected attribution: China

Target sectors: Japanese and Taiwanese organizations in the high-tech, government services, media and financial services industries

Overview: China-based group concerned with Taiwan political and journalistic matters.

Associated malware: IRONHALO, ELMER

Attack vectors: Spearphishing emails sent to Taiwanese media organizations and webmail addresses. Lure documents contained instructions for registration and subsequent listing of goods on a Taiwanese auction website.

Back to top ▵

APT12

Also known as: Calc Team

Suspected attribution: China

Target sectors: Journalists, government, defense industrial base

Overview: APT12 is believed to be a cyber espionage group thought to have links to the Chinese People's Liberation Army. APT12's targets are consistent with larger People's Republic of China (PRC) goals. Intrusions and campaigns conducted by this group are in-line with PRC goals and self-interest in Taiwan.

Associated malware: RIPTIDE, HIGHTIDE, THREBYTE, WATERSPOUT

Attack vectors: FireEye observed APT12 deliver these exploit documents via phishing emails from valid but compromised accounts. Based on past APT12 activity, we expect the threat group to continue to utilize phishing as a malware delivery method.

Back to top ▵

Additional resources

Report – M-Trends 2014: Beyond the Breach

Blog – Darwin's Favorite APT Group

APT10

Also known as: Menupass Team

Suspected attribution: China

Target sectors: Construction and engineering, aerospace, and telecom firms, and governments in the United States, Europe, and Japan

Overview: APT10 is a Chinese cyber espionage group that FireEye has tracked since 2009. They have historically targeted construction and engineering, aerospace, and telecom firms, and governments in the United States, Europe, and Japan. We believe that the targeting of these industries has been in support of Chinese national security goals, including acquiring valuable military and intelligence information as well as the theft of confidential business data to support Chinese corporations.

Associated malware: HAYMAKER, SNUGRIDE, BUGJUICE, QUASARRAT

Attack vectors: This recent APT10 activity has included both traditional spear phishing and access to victim's networks through managed service providers. (For more information on infection via service providers see M-Trends 2016). APT10 spear phishes have been relatively unsophisticated, leveraging .lnk files within archives, files with double extensions (e.g. [Redacted]_Group_Meeting_Document_20170222_doc_.exe) and in some cases simply identically named decoy documents and malicious launchers within the same archive. In addition to the spear phishes, FireEye Threat Intelligence has observed APT10 accessing victims through global service providers.

Back to top ▵

Additional resources

Blog – APT10 Targeting Japanese Corporations Using Updated TTPs

Blog – APT10 (MenuPass Group): New Tools, Global Campaign Latest Manifestation of Longstanding Threat

APT3

Also known as: UPS Team

Suspected attribution: China

Target sectors: Aerospace and Defense, Construction and Engineering, High Tech, Telecommunications, Transportation

Overview: The China-based threat group FireEye tracks as APT3 is one of the more sophisticated threat groups that FireEye Threat Intelligence tracks, and they have a history of using browser-based exploits as zero-days (e.g., Internet Explorer, Firefox, and Adobe Flash Player). After successfully exploiting a target host, this group will quickly dump credentials, move laterally to additional hosts, and install custom backdoors. APT3's command and control (CnC) infrastructure is difficult to track, as there is little overlap across campaigns.

Associated malware: SHOTPUT, COOKIECUTTER, SOGU

Attack vectors: The phishing emails used by APT3 are usually generic in nature, almost appearing to be spam. Attacks have exploited an unpatched vulnerability in the way Adobe Flash Player parses Flash Video (FLV) files. The exploit uses common vector corruption techniques to bypass Address Space Layout Randomization (ASLR), and uses Return-Oriented Programming (ROP) to bypass Data Execution Prevention (DEP). A neat trick to their ROP technique makes it simpler to exploit and will evade some ROP detection techniques. Shellcode is stored in the packed Adobe Flash Player exploit file alongside a key used for its decryption. The payload is xor encoded and hidden inside an image.

Back to top ▵

Additional resources

Blog – Demonstrating Hustle, Chinese APT Groups Quickly Use Zero-Day Vulnerability (CVE-2015-5119) Following Hacking Team Leak

Blog – New Zero-Day Exploit targeting Internet Explorer Versions 9 through 11 Identified in Targeted Attacks

Blog – Operation Double-Tap

Blog – Operation Clandestine Wolf: Adobe Flash Zero-Day in APT3 Phishing Campaign

---

APT1

Also known as: Unit 61398, Comment Crew

Suspected attribution: China's People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department (总参三部二局), which is most commonly known by its Military Unit Cover Designator (MUCD) as Unit 61398 (61398部队).

Target sectors: Information Technology, Aerospace, Public Administration, Satellites and Telecommunications, Scientific Research and Consulting, Energy, Transportation, Construction and Manufacturing, Engineering Services, High-tech Electronics, International Organizations, Legal Services Media, Advertising and Entertainment, Navigation, Chemicals, Financial Services, Food and Agriculture, Healthcare, Metals and Mining, Education

Overview: APT1 has systematically stolen hundreds of terabytes of data from at least 141 organizations, and has demonstrated the capability and intent to steal from dozens of organizations simultaneously. The group focuses on compromising organizations across a broad range of industries in English-speaking countries. The size of APT1's infrastructure implies a large organization with at least dozens, but potentially hundreds of human operators.

Associated malware: TROJAN.ECLTYS, BACKDOOR.BARKIOFORK, BACKDOOR.WAKEMINAP, TROJAN.DOWNBOT, BACKDOOR.DALBOT, BACKDOOR.REVIRD, TROJAN.BADNAME, BACKDOOR.WUALESS

Attack vectors: The most commonly observed method of initial compromise is spear phishing. The spear phishing emails contain either a malicious attachment or a hyperlink to a malicious file. The subject line and the text in the email body are usually relevant to the recipient. APT1 also creates webmail accounts using real peoples' names. While APT1 intruders occasionally use publicly available backdoors such as Poison Ivy and Gh0st RAT, the vast majority of the time they use what appear to be their own custom backdoors. Throughout their stay in the network (which could be years), APT1 usually installs new backdoors as they claim more systems in the environment. Then, if one backdoor is discovered and deleted, they still have other backdoors they can use. We usually detect multiple families of APT1 backdoors scattered around a victim network when APT1 has been present for more than a few weeks.

Back to top ▵

Additional resources

Report – APT1: Exposing One of China's Cyber Espionage Units

Report – M-Trends 2014: Beyond the Breach

SUSPECTED ATTRIBUTION: NORTH KOREA

APT38

Suspected attribution: North Korea

Target sectors: Financial institutions world-wide

Overview: Our analysis of the North Korean regime-backed threat group we are calling APT38 reveals that they are responsible for conducting the largest observed cyber heists. Although APT38 shares malware development resources and North Korean state sponsorship with a group referred to by the security community as "Lazarus", we believe that APT38's financial motivation, unique toolset, and tactics, techniques, and procedures (TTPs) are distinct enough for them to be tracked separately from other North Korean cyber activity.

Associated malware: This large and prolific group uses a variety of custom malware families, including backdoors, tunnelers, dataminers, and destructive malware to steal millions of dollars from financial institutions and render victim networks inoperable.

Attack vectors: APT38 has conducted operations in over 16 organizations in at least 11 countries. This group is careful, calculated, and has demonstrated a desire to maintain access to victim environments for as long as necessary to understand the network layout, required permissions, and system technologies to achieve its goals. APT38 is unique in that they are not afraid to aggressively destroy evidence or victim networks as part of their operations.

Back to top ▵

Additional resources

Report – APT 38: Un-usual Suspects

Blog – APT38: Details on New North Korean Regime-Backed Threat Group

---

APT37

Suspected attribution: North Korea

Target sectors: Primarily South Korea – though also Japan, Vietnam and the Middle East – in various industry verticals, including chemicals, electronics, manufacturing, aerospace, automotive, and healthcare.

Overview: Our analysis of APT37's recent activity reveals that the group's operations are expanding in scope and sophistication, with a toolset that includes access to zero-day vulnerabilities and wiper malware. We assess with high confidence that this activity is carried out on behalf of the North Korean government given malware development artifacts and targeting that aligns with North Korean state interests. FireEye Threat Intelligence believes that APT37 is aligned with the activity publicly reported as Scarcruft and Group123.

Associated malware: A diverse suite of malware for initial intrusion and exfiltration. Along with custom malware used for espionage purposes, APT37 also has access to destructive malware.

Attack vectors: Social engineering tactics tailored specifically to desired targets, strategic web compromises typical of targeted cyber espionage operations, and the use of torrent file-sharing sites to distribute malware more indiscriminately. Frequent exploitation of vulnerabilities in Hangul Word Processor (HWP), as well as Adobe Flash. The group has demonstrated access to zero-day vulnerabilities (CVE-2018-0802), and the ability to incorporate them into operations.

Back to top ▵

Additional resources

Report – APT 37 (Reaper)

Blog – APT37 (Reaper): The Overlooked North Korean Actor

SUSPECTED ATTRIBUTION: RUSSIA

APT29

Suspected attribution: Russian government

Target sectors: Western European governments, foreign policy groups and other similar organizations

Overview: APT29 is an adaptive and disciplined threat group that hides its activity on a victim's network, communicating infrequently and in a way that closely resembles legitimate traffic. By using legitimate popular web services, the group can also take advantage of encrypted SSL connections, making detection even more difficult. APT29 is one of the most evolved and capable threat groups. It deploys new backdoors to fix its own bugs and add features. It monitors network defender activity to maintain control over systems. APT29 uses only compromised servers for CnC communication. It counters attempts to remediate attacks. It also maintains a fast development cycle for its malware, quickly altering tools to hinder detection.

Associated malware: HAMMERTOSS, TDISCOVER, UPLOADER

Attack vectors: APT29 has used social media sites such as Twitter or GitHub, as well as cloud storage services, to relay commands and extract data from compromised networks. The group relays commands via images containing hidden and encrypted data. Information is extracted from a compromised network and files are uploaded to cloud storage services.

Back to top ▵

Additional resources

Report – HAMMERTOSS: Stealthy Tactics Define a Russian Cyber Threat Group

---

APT28

Also known as: Tsar Team

Suspected attribution: Russian government

Target sectors: The Caucasus, particularly Georgia, eastern European countries and militaries, North Atlantic Treaty Organization (NATO) and other European security organizations and defense firms

Overview: APT28 is a skilled team of developers and operators collecting intelligence on defense and geopolitical issues—intelligence that would be useful only to a government. This APT group compiles malware samples with Russian language settings during working hours (8 a.m. to 6 p.m.), consistent with the time zone of Russia's major cities, including Moscow and St. Petersburg. This suggests that APT28

receives direct ongoing financial and other resources from a well-established organization, most likely the Russian government.

Associated malware: CHOPSTICK, SOURFACE

Attack vectors: Tools commonly used by APT28 include the SOURFACE downloader, its second-stage backdoor EVILTOSS and a modular family of implants dubbed CHOPSTICK. APT28 has employed RSA encryption to protect files and stolen information moved from the victim's network to the controller. It has also made incremental and systematic changes to the SOURFACE downloader and its surrounding ecosystem since 2007, indicating a long-standing and dedicated development effort.

Back to top ▵

Additional resources

Report – Russia's APT28 Strategically Evolves its Cyber Operations

Blog – Operation RussianDoll: Adobe & Windows Zero-Day Exploits Likely Leveraged by Russia's APT28 in Highly-Targeted Attack

Blog – APT28: A Window into Russia's Cyber Espionage Operations?

Webinar – APT28: Cyber Espionage and the Russian Government?

SUSPECTED ATTRIBUTION: VIETNAM

APT32

Also known as: OceanLotus Group

Suspected attribution: Vietnam

Target sectors: Foreign companies investing in Vietnam's manufacturing, consumer products, consulting and hospitality sectors

Overview: Recent activity targeting private interests in Vietnam suggests that APT32 poses a threat to companies doing business, manufacturing or preparing to invest in the country. While the specific motivation for this activity remains opaque, it could ultimately erode the competitive advantage of targeted organizations.

Associated malware: SOUNDBITE, WINDSHIELD, PHOREAL, BEACON, KOMPROGO

Attack vectors: APT32 actors leverage ActiveMime files that employ social engineering methods to entice the victim into enabling macros. Upon execution, the initialized file typically downloads multiple malicious payloads from a remote server. APT32 actors delivers the malicious attachments via spear phishing emails. Evidence has shown that some may have been sent via Gmail.

Back to top ▵

Additional resources

Blog – Cyber Espionage is Alive and Well: APT32 and the Threat to Global Corporations

Webinar – APT32: New Cyber Espionage Group

SUSPECTED ATTRIBUTION: UNDISCLOSED

APT5

Suspected attribution: Undisclosed

Target sectors: Regional Telecommunication Providers, Asia-Based Employees of Global Telecommunications, and Tech Firms, High-Tech Manufacturing, Military Application Technology

Overview: APT5 has been active since at least 2007. APT5 has targeted or breached organizations across multiple industries, but its focus appears to be on telecommunications and technology companies, especially information about satellite communications.

Associated malware: LEOUNCIA

Attack vectors: It appears to be a large threat group that consists of several subgroups, often with distinct tactics and infrastructure. The group uses malware with keylogging capabilities to specifically target telecommunication companies' corporate networks, employees and executives.

Back to top ▵

Additional resources

Report – Southeast Asia: An Evolving Cyber Threat Landscape

Report – Nation State and Hacktivist Attacks: Targeted Hits on Asian Organizations

CONCLUSION

Although informative, these documents cannot substitute for thorough intelligence gathering efforts and investigation of suspected cyber attacks. Over the last decade, FireEye has spent over 100,000 hours per year responding to the world's largest and most consequential breaches. This deep incident response experience, gathered from six worldwide security operation centers (SOCs), is curated and fed back into a self-learning, symbiotic security ecosystem that includes over 11 million sensors and is updated every 60 minutes.

FireEye experts, assisted by this ecosystem, track a growing collection of 30+ advanced threat actors and 300+ advanced malware families. They also maintain profiles of 10+ nation-state threat sponsors and 40+ targeted industries to track and analyze financial and political dimensions of cyber threats worldwide. FireEye experts can not only determine the risk associated with a validated threat, but also how the threat got into the environment, how it spread and what can and should be done about it. These insights are delivered as contextual intelligence that helps client organizations quickly prioritize and effectively respond to critical sophisticated threats.

Further reading: Threat Intelligence Reports