# Advanced Persistent Threats (APTs)

mandiant.com/resources/apt-groups

Insight

25 mins read

Advanced Persistent Threats (APTs)

Threat Actors

**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 Mandiant 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.

Additional Resources

**APT35**

Target sectors: U.S. Western Europe, and Middle Eastern military, diplomatic, and government personnel, organizations in the media, energy, and defense Industrial base, and engineering, business services, and telecommunications sectors.

Overview: APT35 (aka Newscaster Team) is an Iranian government-sponsored cyber espionage team that conducts long-term, resource-intensive operations to collect strategic intelligence. Mandiant Threat Intelligence has observed APT35 operations dating back to 2014. APT35 has historically relied on marginally sophisticated tools, including publicly available webshells and penetration testing tools, suggesting a relatively nascent development capability. However, the breadth and scope of APT35's operations, particularly as it relates to its complex social engineering efforts, likely indicates that the group is well resourced in other areas.

Associated malware: ASPXSHELLSV, BROKEYOLK, PUPYRAT, TUNNA, MANGOPUNCH, DRUBOT, HOUSEBLEND

Attack vectors: APT35 typically relies on spearphishing to initially compromise an organization, often using lures related to health care, job postings, resumes, or password policies. However, we have also observed the group using compromised accounts with

credentials harvested from prior operations, strategic web compromises, and password spray attacks against externally facing web applications as additional techniques to gain initial access.

**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.

Additional Resources

**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.

Additional Resources

**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.

Additional Resources

**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: Mandiant 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.

Additional Resources

**APT31**

Suspected attribution: China

Target sectors: Multiple, including government, international financial organization, and aerospace and defense organizations, as well as high tech, construction and engineering, telecommunications, media, and insurance.

Overview: APT31 is a China-nexus cyber espionage actor focused on obtaining information that can provide the Chinese government and state-owned enterprises with political, economic, and military advantages.

Associated malware: SOGU, LUCKYBIRD, SLOWGYRO, DUCKFAT

Attack vectors: APT31 has exploited vulnerabilities in applications such as Java and Adobe Flash to compromise victim environments.

**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.

**APT27**

Suspected attribution: China

Target sectors: APT27 has targeted multiple organizations headquartered around the globe, including North and South America, Europe, and the Middle East. These organizations fall into a range of different industries, including business services, high tech, government, and energy; however a notable number are in the aerospace and transport or travel industries.

Overview: APT27 engages in cyber operations where the goal is intellectual property theft, usually focusing on the data and projects that make a particular organization competitive within its field.

Associated malware: PANDORA, SOGU, ZXSHELL, GHOST, WIDEBERTH, QUICKPULSE, FLOWERPOT

Attack vectors: APT27 often uses spear phishing as its initial compromise method. APT27 threat actors are not known for using original zero-day exploits, but they may leverage those exploits once they have been made public. In at least one case, APT27 actors used a compromised account at one victim organization to send a spear phishing email to other intended victims in the similar industries. Additionally, APT27 may compromise vulnerable web applications in order to gain an initial foothold.

**APT26**

Suspected attribution: China

Target sectors: Aerospace, Defense, and Energy sectors, among others.

Overview: APT26 engages in cyber operations where the goal is intellectual property theft, usually focusing on the data and projects that make a particular organization competitive within its field.

Associated malware: SOGU, HTRAN, POSTSIZE, TWOCHAINS, BEACON

Attack vectors: The group frequently uses strategic web compromises to gain access to target networks and custom backdoors once they are inside a victim environment.

**APT25**

AKA: Uncool, Vixen Panda, Ke3chang, Sushi Roll, Tor

Suspected attribution: China

Target sectors: The defense industrial base, media, financial services, and transportation sectors in the U.S. and Europe.

Overview: APT25 engages in cyber operations where the goal is data theft.

Associated malware: LINGBO, PLAYWORK, MADWOFL, MIRAGE, TOUGHROW, TOYSNAKE, SABERTOOTH

Attack vectors: APT25 has historically used spear phishing in their operations, including messages containing malicious attachments and malicious hyperlinks. APT25 threat actors typically do not use zero-day exploits but may leverage those exploits once they have been made public.

**APT24**

AKA: PittyTiger

Suspected attribution: China

Target sectors: APT24 has targeted a wide variety of industries, including organizations in the government, healthcare, construction and engineering, mining, nonprofit, and telecommunications industries.

Overview: This group is known to have targeted organizations headquartered in countries including the U.S. and Taiwan. APT24 has historically used the RAR archive utility to encrypt and compress stolen data prior to transferring it out of the network. Data theft exfiltrated from this actor mainly focused on documents with political significance, suggesting its intent is to monitor the positions of various nation states on issues applicable to China’s ongoing territorial or sovereignty dispute.

Associated malware: PITTYTIGER, ENFAL, TAIDOOR

Attack vectors: APT24 has used phishing emails that use military, renewable energy, or business strategy themes as lures. Further, APT24 engages in cyber operations where the goal is intellectual property theft, usually focusing on the data and projects that make a particular organization competitive within its field.

**APT23**

Suspected attribution: China

Target sectors: Media and government in the U.S. and the Philippines

Overview: APT23 has stolen information that has political and military significance, rather than intellectual property. This suggests that APT23 may perform data theft in support of more traditional espionage operations.

Associated malware: NONGMIN

Attack vectors: APT23 has used spear phishing messages to compromise victim networks, including education-related phishing lures. APT23 actors are not known to use zero-day exploits, but this group has leveraged those exploits once they have been made public.

**APT22**

AKA: Barista

Suspected attribution: China

Target sectors: A broad set of political, military, and economic entities in East Asia, Europe, and the U.S.

Overview: We believe APT22 has a nexus to China and has been operational since at least early 2014, carrying out intrusions and attack activity against public and private sector entities, including dissidents.

Associated malware: PISCES, SOGU, FLATNOTE, ANGRYBELL, BASELESS, SEAWOLF, LOGJAM

Attack vectors: APT22 threat actors have used strategic web compromises in order to passively exploit targets of interest. APT22 actors have also identified vulnerable public-facing web servers on victim networks and uploaded webshells to gain access to the victim network.

**APT21**

AKA: Zhenbao

Suspected attribution: China

Target sectors: Government

Overview: APT21 leverages strategic Russian-language attachments themed with national security issues in lure documents. Historically, social engineering content is indicative of a cyber espionage operation attempting to gain unauthorized access to privileged information concerning state security in Russia. An analysis of APT21 techniques suggests that another of their focus areas is dissident groups which seek greater autonomy or independence from China, such as those from Tibet or Xinjiang.

Associated malware: SOGU, TEMPFUN, Gh0st, TRAVELNET, HOMEUNIX, ZEROTWO

Attack vectors: APT21 leverages spear phishing email messages with malicious attachment, links to malicious files, or web pages. They have also used strategic web compromises (SWCs) to target potential victims. APT21 frequently uses two backdoors known as TRAVELNET and TEMPFUN. Significantly, APT21 typically primarily uses custom backdoors, rarely using publicly available tools.

**APT20**

AKA: Twivy

Suspected attribution: China

Target sectors: Construction and engineering, health care, non-profit organizations, defense industrial bas eand chemical research and production companies.

Overview: APT20 engages in cyber operations where the goal is data theft. APT20 conducts intellectual property theft but also appears interested in stealing data from or monitoring the activities of individuals with particular political interests. Based on available data, we assess that this is a freelancer group with some nation state sponsorship located in China.

Associated malware: QIAC, SOGU, Gh0st, ZXSHELL, Poison Ivy, BEACON, HOMEUNIX, STEW

Attack vectors: APT20's use of strategic web compromises provides insight into a second set of likely targets. Many of APT20's SWCs have been hosted on web sites (including Chinese-language websites) that deal with issues such as democracy, human rights, freedom of the press, ethnic minorities in China, and other issues.

**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.

**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.

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

**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.

**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.

**APT15**

Suspected attribution: China

Target sectors: Global targets in the trade, economic and financial, energy, and military sectors in support of Chinese government interests.

Overview: APT15 has targeted organizations headquartered in multiple locations, including a number of European countries, the U.S., and South Africa. APT15 operators share resources, including backdoors as well as infrastructure, with other Chinese APTs.

Associated malware: ENFAL, BALDEAGLE, NOISEMAKER, MIRAGE

Attack vectors: APT15 typically uses well-developed spearphishing emails for Initial Compromise against global targets in various sectors that are of interest to the Chinese government. Significantly, APT15 use backdoors and infrastructure that is not unique to the group, making attribution challenging.

**APT14**

Suspected attribution: China

Target sectors: Government, telecommunications, and construction and engineering.

Overview: APT14 engages in cyber operations where the goal is data theft, with a possible focus on military and maritime equipment, operations, and policies. We believe that the stolen data, especially encryption and satellite communication equipment specifications, could be used to enhance military operations, such as intercepting signals or otherwise interfering with military satellite communication networks.

Associated malware: Gh0st, POISONIVY, CLUBSEAT, GROOVY

Attack vectors: APT14 threat actors do not tend to use zero-day exploits but may leverage those exploits once they have been made public. They may leverage a custom SMTP mailer tool to send their spear phishing messages. APT14 phishing messages are often crafted to appear to originate from trusted organizations.

**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: Mandiant 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.

Additional Resources

**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 Mandiant 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, Mandiant Threat Intelligence has observed APT10 accessing victims through global service providers.

Additional Resources

Additional Resources

**APT9**

Suspected attribution: Based on available data, we assess that this is a freelancer group with some nation-state sponsorship, possibly China.

Target sectors: Organizations headquartered in multiple countries and in industries such as health care and pharmaceuticals, construction and engineering, and aerospace and defense.

Overview: APT9 engages in cyber operations where the goal is data theft, usually focusing on the data and projects that make a particular organization competitive within its field.

Associated malware: SOGU, HOMEUNIX, PHOTO, FUNRUN, Gh0st, ZXSHEL

Attack vectors: APT9 was historically very active in the pharmaceuticals and biotechnology industry. We have observed this actor use spearphishing, valid accounts, as well as remote services for Initial Access. On at least one occasion, Mandiant observed APT9 at two companies in the biotechnology industry and suspect that APT9 actors may have gained initial access to one of the companies by using a trusted relationship between the two companies. APT9 use a wide range of backdoors, including publicly available backdoors, as well as backdoors that are believed to be custom, but are used by multiple APT groups.

**APT8**

Suspected attribution: China

Target sectors: A broad range of industries, including media and entertainment, construction and engineering, and aerospace and defense.

Overview: APT8 engages in cyber operations where the goal is intellectual property theft, usually focusing on the data and projects that make an organization competitive within its field. We assess that this is a freelancer group located in China with some nation-state sponsorship. APT8 has targeted organizations headquartered in multiple countries, including the U.S., Germany, the U.K., India, and Japan.

Associated malware: HASH, FLYZAP, GOLFPRO, SAFEPUTT

Attack vectors: APT8 actors often use spear phishing email messages with malicious attachments or links, or it exploits vulnerable Internet-facing web servers to compromise target organizations. In addition, in multiple intrusions APT8 actors sent malicious links to potential victims via chat or instant messaging programs.

**APT7**

Suspected attribution: China

Target sectors: Construction, engineering, aerospace, and defense industrial base.

Overview: APT7 engages in cyber operations where the goal is intellectual property theft, usually focusing on data and projects that make an organization competitive within its field. This group is known to have targeted organizations headquartered in the U.S. and U.K.

Associated malware: DIGDUG, TRACKS

Attack vectors: APT7 threat actors have used access to one organization to infiltrate another organization under the same corporate parent. This is a form of lateral movement, but in this case was also the initial compromise method for the second organization.

**APT6**

Suspected attribution: China

Target sectors: Transportation, Automotive, Construction and Engineering, Telecommunications, Electronic, Construction and Materials.

Overview: APT6 engages in cyber operations where the goal is data theft, most likely data and projects that make an organization competitive within its field. APT6 targeted organizations headquartered in the U.S and U.K.

Associated malware: BELUGA, EXCHAIN, PUPTENT

Attack vectors: APT6 utilizes several custom backdoors, including some used by other APT groups as well as those that are unique to the group.

**APT5**

Suspected attribution: China

Target sectors: Regional telecommunication providers, Asia-based employees of global telecommunications and tech firms, high-tech manufacturing, and military application technology in the U.S., Europe, and Asia.

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. As early as 2014, Mandiant Incident Response discovered APT5 making unauthorized code modifications to files in the embedded operating system of another technology platform. In 2015, APT5 compromised a U.S. telecommunications organization providing services and technologies for private and government entities. During this intrusion, the actors downloaded and modified some of the router images related to the company's network routers. Also during this time, APT5 stole files related to military technology from a South Asian defense organization. Observed filenames suggest the actors were interested in product specifications, emails concerning technical products, procurement bids and proposals, and documents on unmanned aerial vehicles (UAVs).

Associated malware: BRIGHTCREST, SWEETCOLA, SPIRITBOX, PALEJAB, WIDERIM, WINVAULT, HAPPYSAD, BIRDWORLD, FARCRY, CYFREE, FULLSILO, HELLOTHEWORLD, HAZELNUT, GIF89A, SCREENBIND, SHINYFUR, TRUCKBED, LEOUNCIA, FREESWIM, PULLTAB, HIREDHELP, NEDDYHORSE, PITCHFORK, BRIGHTCOMB, ENCORE, TABCTENG, SHORTLEASH, CLEANACT, BRIGHTCYAN, DANCEPARTY, HALFBACK, PUSHBACK, COOLWHIP, LOWBID, TIGHTROPE, DIRTYWORD, AURIGA, KEYFANG, Poison Ivy

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. APT5 has shown significant interest in compromising networking devices and manipulating the underlying software that supports these appliances.

**APT4**

Description:
Also known as: Maverick Panda, Sykipot Group, Wisp

Suspected attribution: China

Target sectors: Aerospace and Defense, Industrial Engineering, Electronics, Automotive, Government, Telecommunications, and Transportation.

Overview: APT4 appears to target the Defense Industrial Base (DIB) at a higher rate of frequency than other commercial organizations. However, APT4's history of targeted intrusions is wide in scope.

Associated malware: GETKYS, LIFESAVER, CCHIP, SHYLILT, SWEETTOOTH, PHOTO, SOGO

Attack vectors: APT4 actors often leverage spear phishing messages using U.S. government, Department of Defense, or defense industrial base themes. APT4 actors may repurpose valid content from government or U.S. DoD web sites within their message bodies to lend them legitimacy.

**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 Mandiant tracks as APT3 is one of the more sophisticated threat groups that Mandiant 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.

Additional Resources

Additional Resources

**APT2**

Suspected attribution: China

Target sectors: Military and Aerospace.

Overview: This group was first observed in 2010. APT2 engages in cyber operations where the goal is intellectual property theft, usually focusing on the data and projects that make an organization competitive within its field

Associated malware: MOOSE, WARP

Attack vectors: Spearphishing emails that exploit CVE-2012-0158.

**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.

**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.

Additional Resources

**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. Mandiant 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.

Additional Resources

**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.

Additional Resources

**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.