NOVETTA

CYBER SECURITY COALITION

EXECUTIVE SUMMARY

TEAM INTRODUCTION

Operation SMN is a coordinated, private-industry effort led by Novetta and supported by a coalition of leading security companies:

- Cisco
- FireEye
- F-Secure
- iSIGHT Partners
- Symantec
- Tenable
- ThreatConnect
- ThreatTrack Security
- Volexity
- An assortment of threat researchers who have wished to remain anonymous

From its inception, the focus of Operation SMN has been to extend beyond the traditional industry status-quo of simply publicizing a report of an identified cyber threat. Instead, we wished to turn knowledge into action. By leveraging the Coordinated Malware Eradication Program, Operation SMN members have synthesized and operationalized shared knowledge of a common threat with the primary objective of disrupting, degrading and globally remediating the effects of a sophisticated, well resourced, cyber espionage group who has operated unabated for at least 4 years.

Novetta feels that the unified approach within Operation SMN is the vehicle in which private industry can effectively come together, collaborate and precisely deliver an effects-based solution for our common customers and the internet as a whole. It is our hope that others will embrace this approach in the future.

To that end, the lessons learned from Operation SMN will be used to further refine the planning and execution of future industry-wide collaborative global mitigation efforts. Future reporting and in-depth analysis of this threat will also include details and metrics of Operation SMN effectiveness.

For the purposes of this document, the threat actors involved will be referred to as “Axiom”.

KEY FINDINGS

- The Axiom threat group is a well-resourced and sophisticated cyber espionage group that has been operating unfettered for at least four years, and most likely more.

- Members of Operation SMN believe that those affiliated with Axiom are physically operating from within China and are conducting espionage activity in support of China’s strategic national interests.

- Axiom operations consist of a variety of generally available implants in addition to highly sophisticated and customized implants to persist undetected within a victim's enterprise for several years.

- Axiom operators leverage an array of compromised mid-point infrastructure within Korea, Taiwan, Japan, Hong Kong and the United States to conduct exploitation operations.

- The Axiom threat group has conducted sustained espionage operations against individuals and organizations that are topically aligned with China's strategic five year plan[1]. Specifically, the group targets organizations that are of strategic financial and economic interest, influence environmental and energy policy, and develop cutting edge information technology (microprocessors) and telecommunications equipment and infrastructure.

- Novetta is confident that the organization responsible for Axiom exploitation activities is an entity operating out of China.

SUMMARY

As early as 2010, and with additional evidence dating back to as early as 2008, Axiom has been responsible for conducting sophisticated cyber espionage operations targeting global Fortune 500 companies, journalists, environmental groups, and public sector organizations worldwide. Axiom traditionally uses spear phishing and strategic website compromises to deliver widely available first stage implants. Once inside an enterprise, the Axiom will leverage hacking utilities for privilege escalation and lateral movement, embedding themselves deeply with complex and customized backdoors and rootkits that are unique to them. Axiom has also been observed leveraging an array of compromised midpoint proxy infrastructure within the United States, Korea, Taiwan, Hong Kong, and Japan, in addition to maintaining supporting infrastructure accounts, such as dynamic DNS services, from a variety of United States and Chinese providers.

PREVIOUS RESEARCH

The Axiom threat group has many similarities with other groups and operations reported on by the security industry in prior years. Because the initial research and analysis of the incidents was insular and conducted independently by organizational security teams, details regarding the incidents were often poorly shared amongst the security industry which generated confusion and debate[2]. Other industry examples which are believed to exhibit subsets of Axiom's motivational, technological, or chronological characteristics are:

- Operation Aurora [3]

- HiddenLynx [4] [5] / Elderwood [6]

- VOHO [7] [8] [9]

- DeputyDog [10] [11] [12]/ Ephemeral Hydra [13]

- ShellCrew [14] [15]

[1] http://www.kpmg.com/CN/en/IssuesAndInsights/ArticlesPublications/Publicationseries/5-years-plan/Documents/China-12th-Five-Year-Plan-Overview-201104.pdf

[2] http://www.securityweek.com/rsa-not-enough-proof-china-behind-elderwood-gang

[3] http://en.wikipedia.org/wiki/Operation_Aurora

[4] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf

[5] http://www.symantec.com/connect/blogs/hidden-lynx-professional-hackers-hire

[6] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/the-elderwood-project.pdf

[7] https://blogs.rsa.com/lions-at-the-watering-hole-the-voho-affair/

[8] https://blogs.rsa.com/voho-apt-campaign-update/

[9] https://blogs.rsa.com/wp-content/uploads/2014/10/VOHO_WP_FINAL_READY-FOR-Publication-09242012_AC.pdf

[10] http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html

[11] http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-part-2-zero-day-exploit-analysis-cve-2013-3893.html

[12] http://www.fireeye.com/blog/technical/cyber-exploits/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html

[13] http://www.fireeye.com/blog/technical/cyber-exploits/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html

[14] https://blogs.rsa.com/dissecting-tactics-techniques-advanced-adversary/

[15] http://www.emc.com/collateral/white-papers/h12756-wp-shell-crew.pdf

Additional information regarding possible linkages will be delivered in future technical reporting.

Axiom actors share a number of similarities with the reported operations and actor sets above. It is important to note that while these actors all show a strong degree of sophistication, and exhibit operational features or tool sets which at times overlap with each other, we are unable to conclusively associate them as a single operational group at this time, and do not suggest that these reports necessarily deal with the same actors as this one. However, the fragmented reporting on these actor groups has made it clear that as an industry we are most effective in countering sophisticated adversaries of this nature when we transparently come together, set corporate agenda aside and share the respective datasets that allow us to develop and act upon the aggregated Threat Intelligence.

BREAKDOWN ALONG THE DIAMOND MODEL OF INTRUSION ANALYSIS

The Diamond Model of Intrusion Analysis [16] is a proven academic model which can be used to organize and associate cyber events, indicators of compromise, and associate context and attributes to one another with certain levels of confidence. In the following subsections we break down the respective Diamond Model vertices to logically separate the characteristics of Axiom.

ADVERSARY

Within the Diamond Model, the Adversary node represents the flesh and bone threat actor, the individual operator(s) behind the keyboard. This may also include the organization(s) in which the actor is affiliated with and/or the direct or indirect benefactor(s) of the malicious activity. When extending the model, the Adversary-Victim relationship can describe the various motivations and intent of the Adversary within a social-political axis.

Based on the scale of Axiom's global compromises, the nature and timing of targeting, the sophistication of the custom malware capabilities leveraged, the advanced exploitation techniques applied, the level of skill, and the operational security observed, only resourced organizations with commensurate time, money and personnel would be capable of carrying out this activity with the degree of efficacy which has been observed by Operation SMN participants.

Members of Operation SMN believe that remote Axiom exploitation operations are being conducted from within China due to observed network patterns, reverse engineering analysis, and victim reports that have been collected. The Axiom group likely consists of multiple groups of operators all responsible for supporting various phases of concurrent global network exploitation and data collection operations. These operators have been observed targeting and collecting information that is seemingly aligned with China's strategic national interests.

VICTIMS

One of the primary methods in determining who an adversary may be and the efficacy of their operations is to conduct analysis of their victims, when they target them, how often they conduct actions on the objective and what they do when inside a target network. As patterns emerge, organizations can begin to infer the motivations of their attackers, applying this knowledge base to a comprehensive security strategy. Over the past four years, Operation SMN members have observed the Axiom actors targeting and exploiting organizations affiliated with the following industries and sectors. All of this information has been sourced using Novetta's reverse engineering capabilities though extraction of binary configurations.

- Finance
- Education & Research
- Government & Defense Industry
- Hi-Technology
- Healthcare & Biomed

[16] http://www.threatconnect.com/files/uploaded_files/The_Diamond_Model_of_Intrusion_Analysis.pdf

- Policy groups & Think Tanks
- Legal
- Media
- Individuals or organizations affiliated with Human Rights, Pro-Democracy, or stand in opposition of the PRC

This adversary maintains a heavy focus on infrastructure within the U.S. in addition to regional targets within Korea, Taiwan, Japan, and Hong Kong. This geographic emphasis is both indicative of the victim set as well as compromised C2 infrastructure and midpoint coordination.

Since September of 2013, Operation SMN members have identified Axiom targeting the following victim types.

- **Human Resource Management Agencies:** Axiom has targeted and exploited U.S. and Japanese government organizations responsible for human resource management.
- **South East Asian Law Enforcement:** Axiom has targeted and exploited individuals and organizations associated with South East Asian Law Enforcement and Ministries of Justice, with an emphasis on Taiwanese-based targets.
- **Environmental Protection & Climate Groups:** Axiom has targeted and exploited individuals and organizations within public and private sectors advocating for and affiliated with environmental protection, multilateral energy & climate policy issues and green technology.
- **Broadcast Media & Journalists:** Axiom has targeted and exploited journalists and media organizations within the U.S., Europe and Japan.
- **International Law Firms:** Axiom has targeted international law firms which facilitate multi-billion dollar international mergers and acquisitions, market access within China, and advise global Fortune 500 companies and major financial institutions.
- **Ministry of Finance & Supervisory Commission:** Axiom has targeted and exploited a Ministry of Finance and an identified regional East Asian Finance Supervisory Commission.

CAPABILITIES

The Diamond Model contains a node reserved for a particular threat's capability. These capabilities describe technical tools and/or techniques that the adversary leverages within a particular intrusion event. Examples of capabilities may be exploit code, custom implants, commonly available utilities or scripts. In extending the model, the Capability-Infrastructure relationship can be used to understand the ways and means in which an adversary leverages Infrastructure to conduct actions on the objective through their respective capabilities. This relationship is commonly known as the technology meta-feature.

In the case of Axiom, the actors will utilize an array of capabilities, some more unique than others, for various phases of their exploitation operations. The following capabilities are general a general list of the backdoors leveraged by this threat.

- Poison Ivy
- Gh0st Rat
- PlugX
- ZXShell
- Hydraq/9002 RAT
- DeputyDog / Fexel
- Derusbi
- Hikit
- ZoxFamily (ZoxPNG, ZoxSMB, etc)

HIKIT GENERATION 1:

Capability Features:

- File management: upload and download
- Remote shell
- Network tunneling (proxying)
- Ad-hoc network generation (connecting multiple Hikit infected machines to create a secondary network on top of the victim's network topology)
- No config stored in sample, no command line parameter passing of C2 (listens for magic bytes)

Interesting Facts:

- Relies on a NDIS (network) driver to communicate between the network and the malware
- The infected machine acts as the server while the controlling machine is the client, therefore at least one Hikit infection must be on an internet facing machine
- Contains no configuration information at all
- The NDIS (network) driver is a mixture of several open source pieces of code, most notably the passthru NDIS driver example from a 2003 blog [17].
- The client authenticates to the server at the NDIS driver layer by providing a specific set of strings that mimic HTTP requests
- Authors routinely forgot to remove the PDB strings revealing at least two compile machines
- Earliest known variants from early 2011

HIKIT GENERATION 2:

Capability Features:

- File management: upload and download
- Remote shell
- Network tunneling (proxying)
- Ad-hoc network generation (connecting multiple hikit infected machines to create a secondary network on top of the victim's network topology)

Interesting Facts:

- Comes in 64-bit and 32-bit versions depending on the target's infrastructure
- 32-bit versions use a rootkit driver to hit the malware process, network endpoints, registry keys and files.
- The rootkit is based heavily on the Agony rootkit which is open source
- Unlike Gen1, the malware acts as a client to the C2's server.
- Uses the same XOR encryption scheme as Gen 1
- Developmental overlap found between Gen 1 and Gen 2 (new Gen1 sample found during the Gen 2 time span)
- Has at least 5 known sub-generations with the Gen 2 lineage
- Spanning from late 2011 to 2013

[17] http://www.wd-3.com/archive/extendingpassthru2.htm

ZOX FAMILY

Capability Features:

- Basic file management: upload, download, create directory, list, write files, delete files, move files, enumeration of attached drives
- Process management: list processes, kill process by PID
- Ability to run arbitrary code from C2
- Remote shell
- Some samples appear to have exploit/spreading capabilities

Interesting Facts:

- Evidence suggests that Zox has variants dating back to at least 2008, and may have multiple generations, and may have evolved from a simple spreader into something a bit more RAT like.
- Uses PNG file format as the carrier format for data to and from the C2
- The sample from 2008 uses SMB to communicate indicating it was originally a local exploitation tool instead of a remote tool
- Does not contain any C2 information as the attacker must provide the information at runtime via the command line
- Evidence in the Zox family of tools suggests a focus on China, Taiwan, US/UK, Korean language sets for exploits offsets leveraged in spreading functionality.
- Was observed being leveraged by attackers via base64 encoded cab file that was then installed via a login script for a specific user. Very few samples have been found compared to all the other malware families the effort is tackling.

DERUSBI (SERVER VARIANT):

Capability Features:

- File management: upload, download, create directory, list files, enumerate entire folder trees, move files, delete files, rename files, get file attributes, mimic timestamps of other files (e.g. copying the timestamp of kernel32.dll to another file to allow for blending in)
- Derusbi may have a windows GUI component for the operator (based on file system behavior, and patterns of use).
- Remote shell
- Basic (limited) network proxying

Interesting Facts:

- Uses a 64-byte handshake of seemingly random data with eight bytes specifically configured to act as the handshake
- The infected machine acts as the server while the controlling machine (the attacker's machine) is a client (the reverse of typical malware communication)
- Does not contain any configuration information related to the attacker's IP, only contains the campaign code
- Appears to be able to co-exist with other running services on the same port

CUSTOM SCRIPTS & UTILITIES

Once inside a target network, Axiom will establish a base of operations and will leverage their initial accesses to escalate privileges targeting key enterprise assets such as domain controllers. Attackers will dump the Security Account Manager (SAM) file or use the Windows Credential Editor to obtain local or domain administrator privileges. Using these administrative privileges the attackers will move laterally, spreading across the enterprise using custom visual basic logon scripts, exploits, scheduled "at jobs" as well as legitimate administrative utilities and services such as Remote Desktop or commercial alternatives.

INFRASTRUCTURE

If Capabilities consisting of the malicious or benign software and utilities are the "ways", then adversary infrastructure is the "means" through which the adversary interacts with their capabilities.

Operation SMN members have identified an overwhelming and comprehensive array of global command and control (C2) infrastructure. The threat actors use this infrastructure as a means of digital mobility, placing distance between their apparent originating source networks and their intended victims. The attackers will also use co-opted infrastructure to conduct strategic website compromises. Generally, throughout various stages of their exploitation operations, the attackers will leverage a discrete toolset, and in some cases exhibit decidedly different C2 patterns. The following patterns and characteristics of threat actor infrastructure have been observed:

China Nexus: Initial waves of binaries created by this threat actor were configured to leverage domain names registered by Chinese registrants using Chinese DNS providers DNS Pod and HiChina.

Rapid Time on Target: Axiom exploitation operations are extremely quick. While conducting data exfiltration operations against organizations within the U.S., attackers have been observed updating dynamic DNS resolutions and "pointing" it to co-opted midpoint infrastructure within the U.S. This technique is likely leveraged in a means to specifically disrupt and confound U.S. law enforcement and Counter-Intelligence operations. The threat is keenly aware of the legal and ethical limitations placed upon domestic surveillance within the U.S. and leverages these laws and policies to its advantage.

Dynamic DNS Usages: The adversary leverages DNS and dynamic DNS services as a means of digital mobility, moving domain resolutions to compromised midpoint C2 infrastructure to disrupt law enforcement, Counter-Intelligence and netDefense mitigation operations. After 2012 there was a general avoidance of U.S. dynamic DNS services within their operations.

Taiwan & Korea Midpoints: Beginning in 2013 Axiom has maintained the bulk of its midpoint infrastructure within Taiwan and Korea. Only when exploiting U.S. victims will the adversary update NS records to activate U.S. based midpoint infrastructure only for a short period of time needed to conduct actions on the objective.

Strict Operational Security: Unlike many other Advanced Persistent Threat (APT) campaigns Axiom stands in contrast, adhering to strict operational security protocols. There has been minimal public evidence of threat actor activity, unlike previously reported activity attributed to Chinese government organizations there have been no observed mingling of individual operators' personal browsing or personal communications on infrastructure used, and there have been no meaningful deviations from their observed operational profile. This adherence to protocol suggests an evolution of a disciplined, well trained, and regimented operations tempo with a strict level of oversight and compliance.

Capability to Infrastructure Configuration: Each Hikit binary is uniquely keyed for each victim with primary and secondary C2 locations and ports of communication configured. Hikit binaries will be configured independently, isolating C2 between targets and rarely sharing common C2 locations. It is believed that this isolation is done as a means to increase attacker survivability. In the event that one campaign or operation becomes compromised, other operations are less likely to be interrupted.

Low Visibility: Between 2012 and 2014 a limited sample set of Hikit has been identified across the five major malware research organizations. Contrasting the Hikit compile dates to passive DNS resolutions suggests that there may be more Hikit samples in the wild than what has been detected via anti-virus, research community, and larger security community efforts.

CONCLUSION

Operation SMN represents a collective industry perspective of a multi-year Chinese cyber espionage operation which has been directed against governments and the worlds largest companies. Irrespective of the many names given to this threat and it's campaigns in previous years, the coalition of Operation SMN members have aligned to proactively disrupt and mitigate this single, persistent threat from countless affected enterprises on a global scale.

Understanding the capabilities and intent of the threat, both technical and socio-political, allows organizations to develop an individualized comprehensive security strategy that is commensurate with the threats that they are likely to face. To that end, individual Operation SMN members will be releasing additional details, signatures and remediations for this threat, giving vendors the opportunity to assist their customers, and victims the ability to defend and remediate their networks.