

Operation SMN:

Axiom Threat Actor Group Report **公理队**

Thank you to our public partners:



















Contents

```
Key Findings – pg. 4
Operation SMN Background - pg. 5
   Operational Impact - pg. 6
Axiom Targeting - pg. 8
   Targeting and China's Strategic Goals - pg. 10
       Semiconductor and Networking Technology – pg. 10
       Human Intelligence - pg. 11
       Non-Governmental Organizations - pg. 11
   Previous Public Reporting – pg. 12
   Domestic Targeting – pg. 15
Tactics, Techniques, and Procedures of Axiom – pg. 18
   Structure of Adversary - pg. 20
       Command and Control (C2) Infrastructure - pg. 21
      Hikit Command and Control (C2) Configuration - pg. 22
Remediation – pg. 23
Kudos - pg. 26
Appendix A: Malware Key Findings – pg. 27
   Hikit Generation 1 – pg. 27
   Hikit Generation 2 – pg. 28
   Zox Family – pg. 28
   Derusbi (Server Variant) - pg. 29
Appendix C: Signatures – pg. 30
      Yara Signature Links - pg. 30
      IDS signatures – pg. 30
Appendix D: Malware Names Index – pg. 30
Appendix E: Malware Hashes – pg. 31
```

Caveats

Operational caveat:

To the best of Novetta's knowledge and belief, participants in this effort did not disclose, access, or utilize any confidential information that would result in violation of any third party agreements, including but not limited to non-disclosure agreements or customer agreements.

Reporting caveat:

Due to the operational sensitivity of this activity and affected organizations, some of the related details will not be included in this report or shared beyond their original sources.

Key Findings

Axiom is responsible for directing highly sophisticated cyber espionage operations against numerous Fortune 500 companies, journalists, environmental groups, pro-democracy groups, software companies, academic institutions, and government agencies worldwide for at least the last six years. In our coordinated effort, we performed the first ever-private sponsored interdiction against a sophisticated state sponsored advanced threat group. Our efforts detected and cleaned 43,000 separate installations of Axiom tools, including 180 of their top tier implants. This report will expand upon the following key findings:

- A coordinated effort across the private sector can have quantifiable impact on statesponsored threat actors.
- The Axiom threat group is a well resourced, disciplined, and sophisticated subgroup of a larger cyber espionage group that has been directing operations unfettered for over six years.
- Novetta has moderate to high confidence that the organization-tasking Axiom is a part of Chinese Intelligence Apparatus. This belief has been partially confirmed by a recent FBI flash released to Infragard stating the actors are affiliated with the Chinese government¹.
- Axiom actors have victimized pro-democracy non-governmental organizations (NGO) and other groups and individuals that would be perceived as a potential threat to the stability of the Chinese state.
- Axiom operators have been observed operating in organizations that are of strategic
 economic interest, that influence environmental and energy policy, and that develop
 cutting edge information technology including integrated circuits, telecommunications
 equipment manufacturers, and infrastructure providers.
- Later stages of Axiom operations leverage command and control infrastructure that has been compromised solely for the targeting of individual or small clusters of related targeted organizations.
- Axiom uses a varied toolset ranging from generic malware to very tailored, custom
 malware designed for long-term persistence that at times can be measured in years. In
 descending order of observed scarcity these families are:
 - Zox family (ZoxPNG, ZoxRPC)/Gresim
 - Hikit
 - o Derusbi
 - Fexel/Deputy Dog
 - Hydrag/9002/Naid/Roarur/Mdmbot
 - o ZXShell/Sensode
 - PlugX/Sogu/Kaba/Korplug/DestroyRAT
 - Gh0st/Moudour/Mydoor
 - Poison Ivy/Darkmoon/Breut

4

¹ http://www.slideshare.net/ragebeast/infragard-hikitflash

Operation SMN Background

Operation SMN² is a coordinated effort amongst leading private-industry security companies, led by Novetta. The initial focus of Operation SMN was to conduct the first industry-led interdiction effort against a sophisticated advanced threat actor group. This collaboration represents an evolution of the status quo from simple reporting of identified threats to a new methodology of coordinated interdiction. During this operation, the group performed malware removal, released detection signatures, and issued public reporting on 10/14/2014³ and 10/28/2014 in order to mitigate the threat posed by the actor group. For the purposes of this document, the name "Axiom" will refer to this threat group.

This effort was initially focused on transferring the understanding generated by Novetta's malware decoder development to Microsoft, via their <u>Coordinated Malware Eradication</u> program, to create high fidelity signatures for the Hikit malware family. These co-developed signatures between Novetta and Microsoft were slated for inclusion in a Malicious Software Removal Tool (MSRT) release that would initially only target the Hikit malware family. Upon the initial few iterations of information sharing and signature development between Microsoft and Novetta it became clear that by leveraging additional industry partners a much larger sample set could be collected, analyzed, and acted upon. This fueled the selective expansion of the partnership into a small group of capable organizations that could contribute directly to the CME campaign.

The expansion of operational scope brought with it discussions of not only targeting the Hikit family of malware, but also refocusing efforts to target the entire known set of associated tools and malware capabilities. It was at this junction that the group decided on a more comprehensive course of action that would leverage the MSRT capabilities for detection and removal, as well as distribute the corpus of samples, analysis, and knowledge to the entire industry via Microsoft's Virus Information Alliance. The group saw that this was the most effective means to broadly distribute highly sensitive information to 64 trusted industry partners in 22 separate countries for their own use, and to protect their customers.

This chain of events enabled Operation SMN members to plan and execute a global disruption and degradation campaign, exposing a Chinese state-sponsored threat actor that has targeted and exploited individual victims and organizations worldwide. Novetta feels that the unified approach developed within Operation SMN, which united multiple perspectives and capabilities across private industry, provides the highest level of visibility and establishes the foundation necessary to effectively counter a threat of this nature. It is Novetta's hope that others within industry will embrace and adopt a similar approach in the future.

http://www.novetta.com/files/5614/1329/6232/novetta_cybersecurity_exec_summary-3.pdf

² http://www.novetta.com/blog/2014/10/cyber-security-coalition1/

Operational Impact

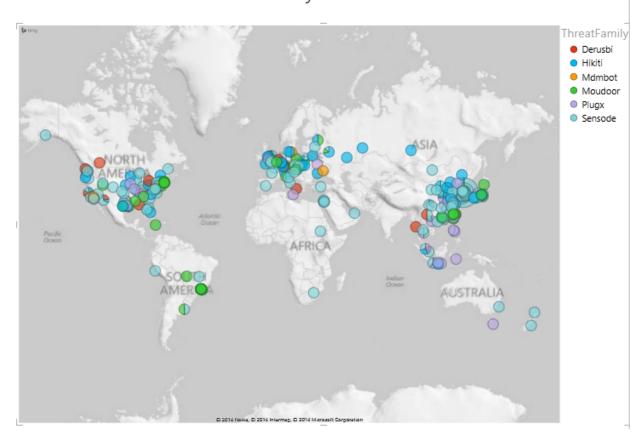
On Tuesday, October 14, 2014, Operation-SMN took its first public action as a Coordinated Malware Eradication campaign (CME-2014-03). This first action consisted of efforts intended to impede the ability of this and other threat actors to leverage this suite of tools. To do so, the coalition:

- Released detection and removal signatures for related malware both publicly and through our coalition partners into their customer bases.
- Provided detection guidance to trusted security partners, including those in the Microsoft Virus Information Alliance program, so that as many potentially affected victims as possible will have detection and protection against this threat.
- Released several stages of reporting designed to raise awareness and highlight the tools, techniques, and procedures leveraged by Axiom and some affiliated groups.

The breadth and scope of Axiom's operations served as motivation and justification for the approach adopted by the coalition of large scale data capture, analysis, and distribution of both data and analytical output to industry. In the intervening period, the coalition has received a substantial amount of information relating to the removal of these malware tools. To date, over 43,000 separate installations of Axiom-related tools have been removed from machines protected by Operation SMN partners, and 180 of those infections were examples of Hikit, the late-stage persistence and data exfiltration tool that represents the height of an Axiom victim's operational lifecycle.

Shown below are two graphs, generated with data from Microsoft's MSRT telemetry, which graph the installation footprint of the various malware samples that Axiom has been observed using. Three clear clusters emerge, centered on what Novetta believes to be areas of responsibility for Axiom. These graphs speak to the usage of a multi-stage corpus of malware which allows the operators to continually refine their targeting as they get closer and closer to their intended goals.

Hikit and Related Family Detections & Infections



Hikit Detections & Infections Around the World



Axiom Targeting

Novetta has observed that Axiom's activity largely centers on using Hikit within victim networks post-compromise. The configuration files extracted from Hikit binaries used in Axiom's operations give identifiable campaign comments that provide strong indications of the intended targets.

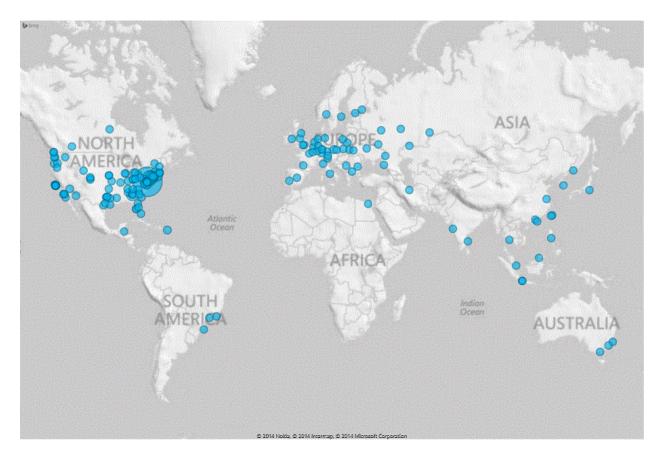
From our analysis, we believe that organizations infected with Hikit are significant to the goals behind those tasking Axiom operations. Though many organizations may have been targeted and compromised with initial stages of implants, the occurrence of Hikit activity within an entity indicates that the organization responsible for Axiom tasking considers it of importance or, alternatively, that the target is relatively hardened and more specialized malware is needed. Within these targets, Axiom has been observed as going out of its way to ensure continued access regardless of changes to its' target's network topology or security controls. Axiom's Hikit operators have been observed returning to compromised organizations on a scheduled basis, and even performing targeted lateral compromises based on the geographic locations of network egress points as well as introduction of new security controls.

Among the industries we observed targeted or potentially infected by Hikit:

- Asian and Western government agencies responsible for:
 - Government records and communications agencies
 - Law enforcement
 - Environmental policy
 - Personnel management
 - Space and aerospace exploration and research
 - Government auditing and internal affairs
- Electronics and integrated circuit manufacturers
- Networking equipment manufacturers
- Internet based services companies
- Software vendors, especially in the APAC region
- Journalism and media organizations
- NGOs, specifically those which deal with human rights or environmental policy
- International Consulting and analysis firms
- Law firms with an international or heavy M&A financial footprint
- Telecommunications firms
- Manufacturing conglomerates
- Venture Capital firms
- Energy firms
- Meteorological Services Companies
- Cloud Computing companies
- Pharmaceutical companies
- Highly regarded US Academic Institutions

These industries cover an array of targeted organizations spanning multiple countries including the United States, South Korea, Taiwan, Japan, and the European Union. Novetta has observed potential compromises from the following geographic areas:

Hikit-Related Passive DNS Activity



Targeting and China's Strategic Goals

Axiom's actions targeting the above industries have fit in particularly well with China's strategic interests and with their most recent Five Year Plans accepted in 2006 and 2011. The 12th Five Year Plan displays China's new direction of pursuing advanced technology and advanced R&D efforts. As China begins its shift away from dependence on foreign technology (specifically the US), more and more corporations and organizations may be targeted by Axiom, and/or other groups that receive the same or similar tasking, as the Chinese play catch-up. The following sections detail how Axiom's Hikit operations line up with official policy.

Semiconductor and Networking Technology

As part of the 12th Five Year Plan, semiconductor and network device manufacturing were two main areas of focus for growth that China has emphasized to minimize foreign dependencies⁴ and increase potential consumption of domestic internet services. Of the many ways the Chinese could acquire this knowledge and technology to further their stated goals, the fastest would be the theft of trade and technology secrets from Western corporations, especially those

⁴ http://www.eetimes.com/document.asp?doc_id=1324373

with offices in China⁵. We have strong indications based on Hikit analysis that these industries have been targeted by Axiom operations.

Human Intelligence

Information on individuals stored by Western and Asian government entities has also been targeted by Axiom. Information held by these organizations includes details on individuals with access to confidential or classified information, which would be extremely useful for intelligence and counterintelligence operations. Additionally, it should be noted that this sort of information could also be used to enable or extend technical and human operations against target organizations and individuals. For example, this can be done through remote network based attacks, tailored spear phishing, targeted social media delivery, physical delivery and transfer of data through non-technical means, and traditional human operations.

Non-Governmental Organizations

Axiom has demonstrated a clear interest in compromising NGOs that deal with international politics, environmental policy, pro-democracy movements, or human rights issues. Novetta has observed at least one operation where Axiom compromised a satellite office of one of these organizations and then appeared to have moved laterally into that organization's main headquarters. Much has been written of China's dissatisfaction of their reputation on the world stage, in particular criticism for human rights abuses and environmental issues stemming from rapid industrialization; these criticisms are often viewed as a blow to the authority of the ruling party and to the "soft power" of their nation state, which China has been keen on developing in recent years. Monitoring these kinds of organizations could allow the Chinese government to track these watchdog organizations and potentially accomplish more traditional goals such as the suppression of dissidents or intimidation of whistleblowers.

-

⁵ http://www.npr.org/2013/05/07/181668369/u-s-turns-up-heat-on-costly-commercial-cyber-theft-in-china

Previous Public Reporting

In addition to the malware binaries that Novetta has analyzed and attributed to Axiom, we have found similarities in several high-profile cyber attacks since 2009. The following timeline details some of the attacks that we know exhibit similar TTPs or leverage overlapping tools and infrastructure with those we have attributed to Axiom.

- June December 2009: Operation Aurora (Hydraq)
- December 2009: Elderwood Project leveraging 0days⁶ (Hydrag)
- March, April June 2011: Elderwood Platform Attacks
- April, May, August 2012: Elderwood Platform Attacks
- June July 2012: VOHO Campaign wateringhole attacks⁷ (Gh0st RAT, Hydraq)
- July 2012 January 2013: Bit9 Compromise⁸, 9 (Hikit)
- June 2013: Shell_Crew Compromise of ColdFusion Server¹⁰ (Derusbi)
- September 2013: Operation Deputy Dog Attack on Japanese Targets¹¹
- November 2013: Operation Ephemeral Hydra involving Internet Explorer Zero-day (DeputyDog)¹²
- January 2014: 3 new 0-Day exploits leveraged by Elderwood Platform¹³
- February 2014: Operation Snowman attack on the US Veterans of Foreign Wars website (DeputyDog)¹⁴
- June July 2014: American Middle Eastern Policy think tank attacks¹⁵

As part of Operation Aurora, Google¹⁶, Adobe¹⁷, Rackspace and 32 other companies were compromised in similar fashion by attackers with connections to China, who we believe exhibit

http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/hidden_lynx.pdf https://blog.bit9.com/2013/02/25/bit9-security-incident-update/

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

⁷ https://blogs.rsa.com/wp-content/uploads/2014/10/VOHO_WP_FINAL_READY-FOR-Publication-09242012_AC.pdf

¹⁰ http://www.emc.com/collateral/white-papers/h12756-wp-shell-crew.pdf

¹¹http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html

¹²http://www.fireeye.com/blog/technical/cyber-exploits/2013/11/operation-ephemeral-hydra-ie-zero-day-linked-to-deputydog-uses-diskless-method.html

¹³ http://www.symantec.com/connect/blogs/how-elderwood-platform-fueling-2014-s-zero-day-attacks

¹⁴http://www.fireeye.com/blog/technical/cyber-exploits/2014/02/operation-snowman-deputydog-actor-compromises-us-veterans-of-foreign-wars-website.html

¹⁵ http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/07/chinese-cyberspies-have-hacked-middle-east-experts-at-major-u-s-think-tanks/

¹⁶ http://googleblog.blogspot.com/2010/01/new-approach-to-china.html

some of Axiom's characteristics¹⁸. Microsoft also reported being subject to similar style attacks, though those attempts were unsuccessful¹⁹. In April 2013, Microsofts' David Aucsmith²⁰ suggested that the Aurora campaign that targeted Google may have been part of a larger Chinese counterintelligence operation aimed at gaining insights to Chinese Gmail accounts which were under FISA (Foreign Intelligence Surveillance Act) surveillance. Later, in May 2013, the Washington Post²¹ would report that according to current and former government officials, the Chinese had successfully accessed Google's database of flagged email accounts that were placed under 702 foreign surveillance by U.S. Law Enforcement and counterintelligence. It is unclear whether these exploitation operations can be directly linked to Axiom, however we have seen direct evidence that Axiom is highly interested in targeting organizations with data that may aid human intelligence or counterintelligence operations.

During the summer of 2012, the VOHO Campaign was discovered by private industry to be leveraging watering-hole attacks and several exploits to download and install variants of Gh0st RAT and Hydraq. The VOHO attacks occurred in two phases, each phase using a different zero-day vulnerability, over multiple weeks during July 2012. According to RSA's reporting on this campaign, nearly 1,000 organizations across multiple industries were impacted during the first phase, resulting in roughly 4,200 individual machines being compromised. During this multi phased attack campaign security firm Bit9 was targeted and Axiom operators gained access to a Bit9 digital certificate. Which they then used to sign custom variants of the Hikit malware in an effort to bypass the additional security provided by their product at specific organizations within the VOHO target set.

The ability to target, compromise, and filter tens of thousands of individual infections across nearly 1000 organizations, in order to identify victims to further other active attacks indicates a level of technical, organizational, and operational sophistication not typically seen. The techniques used and malware delivered in the VOHO Campaign have been tied to Axiom, and the use of digital certificates to deliver malware is also a well-known technique for Axiom.

Watering-hole attacks that include 0-day exploits require planning and sophistication, as the attackers need to identify sites frequented by their targets, compromise those third party website(s), have available 0-day exploits, and then ultimately compromise the visiting targets' systems. Coupling a watering hole attack with a supply chain attack requires even more planning. The fact that the VOHO watering hole attack, the Bit9 compromise, and the delivery of the custom Hikit malware all occurred within a one week period suggests a highly organized

¹⁷ http://blogs.adobe.com/conversations/2010/01/adobe investigates corporate n.html

http://www.wired.com/2010/01/operation-aurora/

http://www.darkreading.com/attacks-and-breaches/google-aurora-hack-was-chinese-counterespionage-operation/d/d-id/1110060?

http://www.cio.com/article/2386547/government/-aurora--cyber-attackers-were-really-running-counter-intelligence.html

²¹http://www.washingtonpost.com/world/national-security/chinese-hackers-who-breached-google-gained-access-to-sensitive-data-us-officials-say/2013/05/20/51330428-be34-11e2-89c9-3be8095fe767 story.html

group able to carry out simultaneous and independent objectives against larger goals, possibly under the direction and supervision of a larger organization.

Another series of attacks named the Elderwood Project²² began in late 2009 and used a notably large number of zero-day vulnerabilities to deliver malware (Hydraq) onto targeted networks. The attackers delivered these exploits using a variety of methods including a watering hole attack targeting the Amnesty International Hong Kong website, which may provide insight into at least some of the victims targeted. The threat actors behind these attacks had access to multiple critical zero-day vulnerabilities, suggesting the group had resources to develop them or to acquire them from other. It should also be noted that the stated techniques of the actors behind Elderwood include targeting of supply-chain organizations of their intended targets.

American think tanks focusing on Iraq have also been targets of watering-hole attacks²³ that utilize malware also occasionally used by the Axiom group: Derusbi. The attack was specifically looking for users with identified Chinese, US English, Russian, Japanese, or Korean language machines²⁴. Although previous Chinese cyber attacks targeting think tanks have concentrated on those involved in East Asian policy, this shift may be reflective of China's renewed interest in the Middle East due to their dependence on oil production from this region²⁵. Although this is not as strong a link to the Axiom threat group, the fact that Derusbi was used is notable, as this malware is not widely distributed beyond intermediate stages of operations that have been attributed to Axiom.

When comparing the last three campaigns that have discussed(VOHO, Elderwood Project, and Iraq-focused think-tanks), beyond the toolset:

- They all used waterholing as their primary initial infection vector
- They all required the ability to sift potentially large sets of infected machines to identify targets of high interest for further exploitation.
- They all targeted (at least in part) non-profit organizations that deal with information related to Chinese policy or Chinese stated interests.

The fact that the primary beneficiary of information stolen in these campaigns is not military or directly financial, but rather intelligence benefiting Chinese domestic and international policies, is highly telling and implies the Chinese Intelligence Apparatus could be behind such attacks.

http://www.washingtonpost.com/blogs/the-switch/wp/2014/07/07/chinese-cyberspies-have-hacked-middle-east-experts-at-major-u-s-think-tanks/

²² http://www.symantec.com/connect/blogs/elderwood-project

http://www.symantec.com/connect/blogs/internet-explorer-zero-day-used-watering-hole-attack-qa http://www.businessweek.com/articles/2014-06-17/iraq-crisis-could-threaten-chinese-oil-investments

Domestic Targeting

In addition to international organizations of strategic interest, it also appears that Axiom has used Hikit internally to gather information on domestic Chinese targets. Cyber operations within China's own borders may be reflective of the Communist Party's emphasis on maintaining internal state security to ensure domestic stability, as the past three decades of rapid economic change have brought about a significant wage gap, unemployment issues, environmental issues, and other societal issues, in addition to long-standing issues such as disparate ethnic groups and territorial disputes. The CPC has subsequently dedicated significant resources toward domestic security: although domestic security spending for 2014 was not revealed by official sources, in the three years prior it has consistently exceeded the military budget²⁶. Among the well-funded entities tasked with domestic security are the Ministry of Public Security and the Ministry of State Security. In particular, the latter organization is the primary non-military security agency of China and is tasked with not only domestic surveillance, but also foreign intelligence and counterintelligence.

Much of previous public reporting on Chinese threat groups has concentrated on the cyber capabilities and information warfare of the People's Liberation Army (PLA). In particular, the Third Department serves as the PLA's telecommunications reconnaissance bureau charged with SIGINT for foreign intelligence operations²⁷. The Third Department is divided into twelve bureaus, each ostensibly having a dedicated mission. For instance, the 2nd Bureau, or Unit 61398, has been directly linked by security researchers to attacks primarily focused on Englishlanguage organizations of strategic importance to China²⁸. While this group has been responsible for a significant number of cyber attacks, the group's profiled operational security and tactics do not appear to be as sophisticated as those attributed to Axiom. In fact, researchers were able to directly link individuals to this bureau due to activity on social media as well as identifiable indicators used to register campaign command and control (C2) infrastructure, including domains or emails. Other individuals linked to Unit 61398 cyber operations have also been profiled by the FBI in an indictment of five Chinese military intelligence officers²⁹. In contrast, there have been no identified mistakes in operational security on the part of Axiom operators to date.

Other attacks targeting satellite/aerospace industries have been linked to the Third Department's 12th Bureau, Unit 61486³⁰. Again, at least one individual has been connected to this activity using open-source intelligence due to a presence on social media and clues found in campaign infrastructure information, suggesting a lax operational security when compared to

²⁶ http://www.trust.org/item/20140305043104-x0f0c/0

http://project2049.net/documents/countering_chinese_cyber_operations_stokes_hsiao.pdf

²⁸ http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf

http://www.fbi.gov/pittsburgh/press-releases/2014/u.s.-charges-five-chinese-military-hackers-withcyber-espionage-against-u.s.-corporations-and-a-labor-organization-for-commercial-advantage
http://www.crowdstrike.com/blog/hat-tribution-pla-unit-61486/index.html

what has been observed with Axiom. Furthermore, attack activity from Unit 61486 has been linked to Unit 61398 based on shared infrastructure. This might suggest some degree of cooperation or overlap between these teams and missions in the Third Department that we have not yet observed between previously identified Chinese threat groups and Axiom, beyond the usage of commonly available malware. However, we cannot discount the possibility that previously reported Chinese threat groups could be linked to Axiom, or that both could be part of a larger organization.

While it appears that the identified missions of most if not all units of the Third Department remain focused on foreign intelligence and defensive network security, there are some indications that a few PLA bureaus do engage in unconfirmed domestic monitoring to some degree, including monitoring of domestic broadcasts. Nevertheless, based on observed TTPs of identified PLA threat groups compared to Axiom activity, we believe that Axiom operates based on a different mission and has resources that previously reported and identified PLA cyber operators do not have.

When examining Axiom's possible domestic attack activity, we have identified several instances of Hikit present on machines located in China or Hong Kong, dating at least as far back as January 2012. This would indicate domestic monitoring in addition to foreign operations, and may suggest that the group to which Axiom belongs is an entity charged with domestic security.

Additional telemetry we have observed suggests that Axiom may also target Chinese citizens, possibly dissidents, in foreign countries (including the United States and Asia-Pacific countries), based on the presence of Hikit on machines configured to use simplified Chinese. In particular, at least one Hikit sample was observed targeting a Chinese-language machine located in the United States; the filename "LiulanqiXunzhang.exe.tdl" appears to reference a browser (浏览器).

Certain indicators from Hikit binaries detected on machines in China or Hong Kong also provide further insight how these domestic victims are targeted by Axiom. The filenames of the malware, for instance, show that they were likely curated for Chinese speakers, as seen with Chinese-language file names including at least one referring to QQ, the popular messaging application. Other more generically popular applications like Adobe Flash Player were also used as potential lures or means of hiding in plain site. Novetta has also observed that Chinese-related filenames of commodity malware that has been used by both Axiom as well as other threat groups (e.g., Poison Ivy, PlugX, etc.) may also reflect a lively underground trade; some of the filenames we have observed are listed below.

Table: Filenames of some malware binaries present on machines located in China

| Original Filename | Translation | Malware Family |
|--|---|----------------|
| QQ6.3_6.3.12382.exe.P2P | | Hikit |
| baofeng.exe.td | | Hikit |
| CODOL_Formal_1.2.2.10_1. 2.2.12_1550_1D.exe.ttd ³¹ | | Hikit |
| LOL_V3132_1151_8D.exe.ttd | | Hikit |
| install_flash_player_ax_KB37 0237.exe.P2P | | Hikit |
| BDWebAdapterZip.dll.bdl | | Hikit |
| QQsetup.exe | | PlugX |
| www.0716che.com | | PlugX |
| www.6541601.com | | PlugX |
| www.6794945.com | | PlugX |
| ARP 扫描 .rar | ARP scanner | ZXShell |
| 各大0day.zip | Major 0day | ZXShell |
| 兄弟网络三版 1433.exe | Fraternal Network ³³ Third Edition 1433 | ZXShell |

Although this information does not conclusively determine that Axiom conducts such operations, when compared with some binary file names it could indicate deliberate targeting.

Additionally, Axiom has used at least one Chinese companies' certificate to sign a Hikit binary: 安微科大讯飞信息科技股份有限公司 (Anwei iFLYTek Information Technology Co. Ltd.), which specializes in voice recognition software and is owned in part by China Mobile, a State asset. While we do not know if domestic companies were compromised for Axiom's purposes or, alternatively, have cooperated with Axiom campaigns, it again suggests Axiom ability and potential desire to stage domestic operations. Other Chinese companies as well as popular Asian gaming companies have also been used to digitally sign malware samples.

33 Might refer to the website hackxd .com (兄弟网络技术论坛, Fraternal Network Technology Forum)

³¹ Likely posing as the game Call of Duty Online

³² Likely the online game League of Legends

In addition to Hikit, we have observed other Axiom-related malware targeting domestic organizations, including a few universities and research institutions in both Hong Kong and mainland China. Though this cannot be linked conclusively to Axiom Hikit operators, education institutions, particularly those in Hong Kong, would likely be of extreme importance for any monitoring of domestic activity -- not only is China worried about liberal academics, but also students, who have historically been leaders in pro-democracy movements as recently as this past summer with the Occupy Central protests in Hong Kong.

Tactics, Techniques, and Procedures of Axiom

A wide range of mechanisms are used to reach the stage of an operation where Hikit is deployed. Observed methods include the traditional use of spear phishing, leveraging of generic and strategic website compromises, and targeted attacks against public facing infrastructure. One of the many disturbing attributes of Axiom and their affiliated groups is their ability to create and leverage large pools of compromised machines, sift through them to identify the organizations of interest, and quickly (within hours or days) begin secondary follow-up exploitation operations. This rapid transition from identification to action on the objective demonstrates the level of sophistication and focus of these actors; it also suggests an integrated targeting element, with possible inputs from an authoritative tasking entity, which is responsible for issuing dynamic taskings. This modus operandi does not suggest that Axiom relies solely upon casting a large net for victimization, rather that the Axiom actors have a well-established tradition and capabilities that support focused targeting of both individuals and organizations.

Once inside an enterprise, Axiom begins reconnaissance almost immediately to establish where they are in the target's network, and to identify any changes that have been made to the environment. Once this initial reconnaissance stage has been completed and the information is collected, Axiom typically moves quickly to escalate privileges on compromised machines via previously compromised administrative accounts, local exploits, or remote exploits as demonstrated in the ZoxRPC malware. This escalation of privileges is typically in an attempt to dump the latest credentials they can gain access to on the victim network. This information is quickly accessed, compressed, encrypted, and exfiltrated by the actors. The turnaround for the use of this information after collection can vary from minutes to months.

The Axiom threat actor group has also demonstrated the operational flexibility of leveraging systems administration tools available within targeted organizations (e.g., Remote Desktop Protocol (RDP), remote administration tools). It has been observed several times that Axiom operators have even leveraged these capabilities as a means of maintaining additional persistence via setting "sticky keys" for RDP sessions. They also use custom tools containing network and local exploits, hacking utilities, and legitimate security tools for privilege escalation and lateral movement. By leveraging tools already available within a target organization Axiom, can forgo the need to potentially raise their profile by deploying additional malware that may trigger antivirus or IDS indicators. As a typical scenario when compromising an organization, this actor group will aim to orient themselves, move laterally, escalate privileges, dump

credentials, and install other families of malware to hedge against detection of any one variant of their malware.

It has been observed in many of Axiom's victim environments that the total number of malware families leveraged can exceed four separate "layers" of malware. These families of malware range in uniqueness from extremely common (Poison Ivy, Gh0st, ZXshell) to more focused tools used by Axiom and other threat groups directed by the same organization (Derusbi, Fexel) to tools only seen used by Axiom (ZoxPNG/ZoxRPC, Hikit). This is likely done to ensure a certain level of persistence and redundant command and control should one of the families ever become compromised. Additionally, once into later stages of their operations, Axiom operators will create and deploy shell utilities that are customized to the operational environment. Operators will also install data archival and compression tooling that may not already exist on the target machine. The flexibility and fluency of Axiom's toolset, including the ability to produce custom tools, is yet another indicator of the technical and operational sophistication of this entity.

In support of this flexible tooling capability, Axiom has demonstrated a relatively sophisticated use of large amounts of legitimate and compromised internet infrastructure. Axiom has been observed grooming and leveraging an array of compromised proxy infrastructure within the United States, South Korea, Taiwan, Hong Kong, and Japan. Novetta has observed indications in various datasets that this compromised infrastructure can be created per campaign or target, or can be shared within a cluster of related targets. It is surmised that this method is a means to create confusion for any investigation into activity related to an Axiom intrusion, by leveraging the capabilities of Axiom tools and interweaving legitimate traffic to the same IP address during the compromise. The net effect of this tactic is to create a set of network traffic that at first glance appears to be legitimate traffic.

Beyond this generally stealthy technique for hiding malicious traffic, the ability to have access to a continual pool of compromised infrastructure in which to overlay their operations speaks to the ability of Axiom actors. They do not just comprise various Internet facing platforms, but also have the organizational ability to deal with the capture, grooming, and maintenance of a large set of compromised infrastructure while in parallel executing technical operations and creating new targeting information for pursuit. On top of Axiom's usage of compromised infrastructure they also maintain supporting infrastructure accounts, such as dynamic DNS services, and VPS/hosting providers from a variety of United States and Chinese providers. This ability to leverage both compromised and legitimate infrastructure enables Axiom to adjust to a target's security posture and potentially extend their access to a targeted organization.

Victim Life Cycle

Based on observed victim environments infiltrated by Axiom, Novetta believes that there are at least six separate tiers of responsibilities that service different stages of the victim lifecycle.

Axiom, for its part, largely conducts operations in later stages of the overall victim compromise. Currently, we believe that the victim lifecycle is split into the following stages:

- Stage 0: Target identification and reconnaissance
- Stage 1: Initial access, validation and internal target reconnaissance
- Stage 2: Lateral movement, and creation of additional footholds
- Stage 3: Compromised infrastructure creation and grooming
- Stage 4: Stealthy identification and exfiltration of targeted data
- Stage 5: Maintain access and understanding of environment

The level of sophistication seen by this multistage life cycle implies a number of things about the adversary's ability to command resources and coordinate within itself. It is this structure and coordination that truly sets Axiom and its associated groups apart from other actors in this space.

Structure of Adversary

We also assess that different groups associated with the Axiom threat actor group likely perform various phases. This deduction is supported by the number of differences in the observed activity during these compromise stages which suggest a number of separate teams with varying responsibilities during their operation lifecycle. For instance, examinations of differences in command and control (C2) and midpoint proxy infrastructure displayed by the Stage 1, Stage 2 and Stage 4 binaries have led us to believe that the operational tempo, security policies, and acceptable risk levels are drastically different. This coordination of different operators, infrastructure, and tools between stages in the same environment suggests a common operating picture within a large organization.

It cannot be overstated that the operational timelines observed imply that Axiom and other stage operators operate with a cohesive long-term strategic goal. The ability of any organization to consider strategic objectives over a multi year period implies that organization both believes that their operations will have far reaching effects, and that the organization itself will exist for an extended time. Extended operations require meaningful resources, both in terms of financial capital (salaries), as well as physical resources (money for VPS's and traditional server infrastructure), as well as a logistic overhead for coordinating, planning, and researching attack vectors, creation/purchasing and distribution of 0-day exploit code and associated exploit frameworks³⁴, and campaign coordination between subgroups.

Finally, threat actors at all the described stages, including Axiom, display a clear level of discipline in using their compromised resources. There is no meaningful level of information leakage due to resource access, or due to visiting personal websites with these resources. While this level of discipline has been observed outside of governmental organizations and

³⁴ http://www.svmantec.com/connect/blogs/how-elderwo<u>od-platform-fueling-2014-s-zero-day-attacks</u>

funded operations, it displays a level of familiarity with investigative and forensics operations that clearly sets them apart from the less sophisticated threat actors.

Command and Control (C2) Infrastructure

The infrastructure practices of these linked groups often change depending on the current stage of operation as well as the intended target, ultimately culminating in Axiom operations. A good example would be the watering hole attacks observed targeting Japanese entities in 2013³⁵. Because broad-spectrum watering hole attacks are widely noticed and reported on, Stage 1 operators appear to have heavily segregated their infrastructure from the infrastructure used during later stages of operation in order to better evade detection.

Operation SMN partners have a great deal of insight into the network characteristics and C2 of the Stage 2 tools and techniques (i.e., Derusbi, HyDraq, DeputyDog) which serve as secondary persistence and lateral movement tools. Here, unlike Stage 1, the tools frequently reuse infrastructure and other resources, and there is even some historical overlap between second level domains used by the Stage 2 actors and the Stage 4 operators (Axiom). iSIGHT Partners' reporting has discussed the usage of domains in watering hole attacks that have been used to gain initial access to target networks for later stage persistence. Passive DNS analysis has demonstrated that the linkages between Stage 2 and Stage 4 C2 domains are indirect, but present, establishing a possible link between the stages. Unlike other threat actors, operators of all stages, particularly from Stage 3 onwards, take operational practices and security seriously. There was no observed activity outside of campaign activity on the identified operational infrastructure across 76 unique Stage 4 campaigns.

For Stage 3 and 4 operations, Axiom is believed to have established a complex C2 infrastructure, which, based on campaign identifiers extracted from configuration files embedded in Hikit binaries, has been used to manage at least 76 unique campaigns that this operation has discovered. Operation SMN partners believe that many more organizations have been affected by Axiom, but are currently unaware of any compromise due to Axiom's hyper targeting and stealth at this stage of activities. We hope that by highlighting some of Axiom's techniques, tactics, and procedures we will increase the visibility of this group for awareness and detection.

The curated infrastructure that appears to be used strongly suggests that the Axiom actors are given the capacity and mandate to target and develop long-term strategic assets. Within observed compromises, Axiom actors have been seen performing complex actions with their C2 infrastructure during the Stage 4 operational cycle. Configuration files extracted from Hikit binaries indicate that C2 callback locations are tailored to the specific country and network environment in which the target resides. C2 domains will consistently be named and hosted in such a way that traffic appears legitimate, likely in an effort to fool network security operators of target organizations. Axiom and its linked groups have been known to conduct extensive research prior to compromising a target in order to determine ideal hosting locations. To achieve

21

³⁵ http://www.fireeye.com/blog/technical/cyber-exploits/2013/09/operation-deputydog-zero-day-cve-2013-3893-attack-against-japanese-targets.html

this, these threat actors often compromise secondary targets in order to obscure their C2 infrastructure and data exfiltration endpoints from their intended victims.

Additionally, past attacks have displayed that these linked groups are capable and willing to construct supply-chain attacks to allow them access to hardened targets. These supply-chain attacks will extend to elements of the target's security supply chain. The observed tempo in these supply-chain attacks suggest that Axiom operators are capable of coordinating rapid responses to roadblocks in their goals, even when those roadblocks represen sophisticated security organizations, such as Bit9.

Hikit Command and Control (C2) Configuration

Axiom's rather distinct network operations and TTPs for setting up C2 infrastructure separate them from other threat actors. In particular, Axiom's midpoint centric C2 infrastructure has resulted in unique fingerprints. Each Hikit binary is configured for a specific target, often included in or referenced within the campaign indicator field of the respective configuration file. Hikit operators (Axiom) appear to use a significant amount of C2 infrastructure isolation between targets, with different targets rarely sharing identical C2 locations. This isolation provides a high degree of resiliency and operational security in the event that one operation becomes compromised, other operations are less likely to be interrupted or affected.

It is important to note that prior to Hikit Generation 2, we have no direct evidence of any C2 infrastructure due to the nature of Hikit Generation 1's functioning. During the transition between the Generation 1 and Generation 2 codebases, Hikit development teams made the decision to include an embedded configuration file in the binary itself. The first evidence of Hikit samples containing this configuration information, with embedded C2 information, appears to have been initiated on April 12, 2012.

During this time, two stages of Hikit binary creation were observed. During their initial stage of work (those binaries with compile dates prior to April 2012), Axiom appeared to use both traditional DNS hosting services and dynamic DNS services equally. While Axiom did not appear to have any obvious criteria for deciding which DNS provider would be used during this period, a preference for using DNSPOD (a Chinese-based DNS provider) and DtDNS (a US-based dynamic DNS service) was clear. The reasons for the selection of DtDNS are unknown at this time but, the selection of DNSPOD can be assumed to be due to the geographic location of the provider itself. The use of Dynamic DNS services is interesting, due to the confounding effect that it generally has on investigations. After 2012, however, we have observed a general avoidance of dynamic DNS services.

Naming conventions of these Hikit domains is also notable due to the pattern that defines them. Under almost all conditions, the domains are expressed as a 3LD format, where the youngest child domain represents the intended campaign target. As an example, the domain format for Acmelnc would be 'acmeinc.basedomain.tld'. This naming convention, as well as the usage of DNS providers, is exclusive to Stage 4 infrastructure. In fact, for all Stage 3 cases, no second level domain is directly used. Instead, whenever malicious activity is observed, it can only be

strongly correlated to the child domain (of the DNSPOD domains), while the second level domain remains relatively static and 'clean' in Asian geographic locations.

Historical examination of the base second level domains base, however, suggests that the second level domains were once used to launch attacks, similar to those domains seen in Stage 2 operations. As this activity was last observed in 2010, it is theorized that current operational strategies were then developed and adhered to.

As noted above, most of the observed Hikit (Stage 4) campaigns rely on DNS services for C2 location and coordination. While the A records for the child domains of the mothership (second level domain) DNS names are typically located on compromised infrastructure as previously discussed, there are a few identifying characteristics which have been noted. Firstly, these domains have extremely short times of existence within the US. Secondly, they display "long distance relationship" behavior, wherein they have NS records in countries outside the location of the child domain. Heuristic detection for candidate C2 domains involves looking for domains that have had RDATA that exhibits travel between geographically disperse countries, and correlating that towards displayed naming and linguistic characteristics of the domain names. Hikit binaries have also been observed as members of complex internal routing structures for the purposes of stealthy data exfiltration as well as access and persistence to internal resources. This activity is rarely caught in practice, as many security teams neglect to perform flow analysis on internal-to-internal network traffic.

At all points during Axiom Stage 4 infections, evidence suggests that there are humans directly orchestrating operations. Stage 1 and Stage 2 operations may have varying levels of human involvement. As a result, exhaustive lists of domain names and IP's used in C2 operations are somewhat useless; blacklisting will be ineffective and present a large amount of 'collateral damage' due to the use of compromised infrastructure. Interestingly, despite the general usefulness of large scale passive DNS analysis in most threat research, there are indications that many of the 'hits' for Axiom C2 domains in this research exist because of independent security researchers or IT security teams conducting investigations. This activity, while reliable for observing network C2 behavior, does make 'operational end dates' difficult to determine for Stage 3 and 4 campaigns.

Remediation

Currently, organizations that wish to protect themselves from the malware that Axiom has been observed using should download and utilize the latest MSRT release. This tool has been verified to provide protection against malware families that Axiom favors, and is freely available to all Microsoft installations. It is suggested that enterprise organizations push out and execute MSRT on a monthly basis. Additionally, all members of the Operation SMN group have up-to-date signatures and heuristics for detecting the Axiom malware families, as well as any vendors involved in Microsoft's VIA program.

It is strongly advised that organizations seeking protection from Axiom avoid the temptation of solely deploying network based signatures. Because Axiom continually creates new C2 infrastructure for each new target and can quickly transition to new malware tooling, it is very unlikely that existing network IOCs will offer any meaningful level of protection for organizations whose infections are new or previously undiscovered.

Network operators can and should learn from the Axiom group's tradecraft; security teams and IT staff should be especially wary of any traffic going to destination servers that does not match the apparent intent of these servers. For example, large data transfers moving towards DNS nameservers on port 53 with no observable DNS content that are associated with known or related partners should be viewed as suspect. Hikit's usage of internally routed proxy nodes can complicate this task, and only advanced network analytics that includes a holistic view of internal and external network traffic can provide anything near 100% certainty. Network boundaries of all types should be monitored. If an internal network can route from restricted zones to ones of lower restriction, it should be monitored for data exfiltration in the same manner as a traditional border network. Above all there is absolutely no substitute for continued vigilance -- by the time Hikit is installed on a victim's infrastructure, the operation is in its final stages, and the attackers generally have free reign over the victim network.

Enterprises are advised that while Axiom represents an advanced attacker, their power comes from their discipline and logistics. Ultimately, the removal of common "low hanging fruit" in network and endpoint security will go far to prevent Axiom from easily accessing networks. Additional suggestions for protection against Axiom's attacks would be:

- Block or sinkhole the DNSPOD name servers. DNSPOD seems to be the preferred provider for DNS services for Axiom, and many organizations can block these resources without adverse effect on business needs.
- Install and execute Microsoft's EMET on endpoint machines, and configure it to your environment.
- Globally edit Windows policies to disable the "Sticky Keys" functionality.
- Restrict all remote access (RDP, SSH, Citrix, VPN, etc.) and ensure that this access is only given to people that need it versus by default for the whole company; wherever possible, implement two-factor authentication for any remote access.
- Keep strong monitoring on VPN endpoints -- Axiom has demonstrated the ability to enter networks after compromising VPN client user credentials.
- Two-factor protection to webmail services should be added where possible.
- Ensure that local administrative accounts are not universal across your network, as a single compromise can bring the security of the entire network into question. Ensure that local firewalls are configured and restrict access to both servers and workstations to only those subnets and users that require it.
- Implement application whitelisting to prevent execution of unauthorized executables -Microsoft AppLocker, Bit9, and other third party solutions are all improvements over
 default installations without whitelisting.
- Encrypt e-mail where possible, even between internal users.

- Ensure antivirus software is reporting to a central, monitored location. Axiom's binaries can flag AntiVirus rules that end up ignored, a security failing that they rely on.
- Ensure proper auditing and review of security firewall rules, antivirus updates, IDS signatures, and other security controls. Axiom actors during active compromises have been observed to disable key signatures or rules to force victim organizations to lose visibility.
- Apply security patches in a timely manner. While Axiom does make use of 0-day vulnerabilities, the group has also used disclosed, patched vulnerabilities that are found on outdated systems in a target's network.
- Reference information provided by the FBI in their FLASH report additional remediation information and suggestions are included ³⁶.

25

³⁶ http://www.slideshare.net/ragebeast/infragard-hikitflash

Kudos

Operation SMN and the subsequent actions taken by the group members could not have occurred without the generosity and talent of several organizations. While the publicly acknowledged members of the group made critical contributions there are other firms that were critical to the findings contained in this report. Their datasets, services, and software allowed coalition members to construct a substantially stronger case than would have been otherwise possible. Farsight Security generously provided Novetta with unrestricted access to their historical passive DNS dataset, allowing analysts to investigate the C2 infrastructure used by Axiom over a wide window of time. Endgame provided Novetta with extensive proprietary threat data and analytical processing capabilities allowing Novetta to gain a deeper insight into compromised network footprints. Novetta would also like to thank those organizations and individuals who quietly contributed to the content covered in this report.

Appendix A: Malware Key Findings

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
- Hydrag/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 blog³⁷.
- 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

³⁷ http://www.wd-3.com/archive/extendingpassthru2.htm

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

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 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 four 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 [unconfirmed, but speculated based on network capture evidence]

Appendix C: Signatures

Yara Signature Links:

Signatures from Novetta and ThreatConnect can be directly downloaded from the following sources:

http://www.novetta.com/operationsmn

IDS Signatures

As detailed here³⁸, Cisco, as a member of the overall coalition has released IDS signatures for their products.

Similar signatures that cover the tools used by axiom can be obtained via the EmergingThreats open signature set below³⁹. Novetta is working with both partners to insure that the signatures they have provide the best coverage possible.

Appendix D: Malware Names Index

| Operation SMN Name | Other Industry Names |
|--------------------|--|
| Hydraq | McRat, HydraQ/HidraQ, Naid, Homux, HomeUnix, MdmBot, Roarur |
| Gh0st | Moudoor, Mydoor |
| PlugX | Korplug, Sogu, Kaba, DestroyRat, TVT, Thoper |
| Poison Ivy | Breut, Darkmoon |
| Derusbi | Photos, Etso, Ocrums, win32.Agent.dbwr |
| Hikit | Hikiti |
| Fexel | DeputyDog |
| ZoxPNG | gresim |
| ZoxRPC | |

http://blogs.cisco.com/security/talos/threat-spotlight-group-72/
 http://emergingthreats.net/products/etpro-ruleset/daily-ruleset-update-summary/

Appendix E: Malware Hashes

To the best of our abilities, Novetta has filtered some of the sample hashes collected from the below sample hashes. This has been due to the highly targeted nature of some of the malware samples Operation SMN has collected. The defensive value of knowing those samples or the hashes for organizations other than the targeted is nil given the technical information produced and shared by this effort. The below hashes are for sample families that leverage shared generic infrastructure between multiple compromised infrastructure or contain no configuration information in the binary.

Links:

http://www.novetta.com/operationsmn