Symantec

SECURITY RESPONSE

Hidden Lynx – Professional Hackers for Hire

Stephen Doherty,
Jozsef Gegeny,
Branko Spasojevic,
Jonell Baltazar

Version 1.0 – September 17, 2013

"The Hidden Lynx group is a professional team of attackers with advanced capabilities."

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

CONTENTS

OVERVIEW

The Hidden Lynx group is a professional team of attackers with advanced capabilities. They were responsible for the compromise of security firm Bit9's digital code-signing certificate which was used to sign malware. The Bit9 breach was part of the much larger VOHO campaign and that campaign was just one of many operations undertaken by the group over the last four years.

The group likely offers a "hackers for hire" operation and is tasked with retrieving specific information from a wide range of corporate and government targets. They are a highly efficient team who can undertake multiple campaigns at once, breach some of the world's best-protected organizations and can change their tactics quickly to achieve their goal. They usually attack using multiple customized Trojans designed for specific purposes. Backdoor.Moudoor is used for larger campaigns and has seen widespread distribution while Trojan.Naid is reserved for special operations against high value targets. The group uses cutting-edge attack techniques which makes this team stand out from other major attack groups.

This paper takes an in-depth look at the Hidden Lynx group, their targets and their motivations. It will look into their capabilities and attack strategies through their attack campaigns including the Bit9 incident.

Symantec

BACKGROUND

> “A well-known group with affiliations to “Operation Aurora” managed to break into Bit9’s network using an SQL injection attack.”

Background

In February 2013, Bit9 released a statement revealing that in July 2012, their network had been compromised by a malicious third-party. A well-known group named Hidden Lynx with affiliations to "Operation Aurora" managed to break into Bit9's network using an SQL injection attack. These Trojans made their way into the defense industrial sector.

However, the Bit9 compromise was only a small piece of a much larger watering-hole operation known as the VOHO campaign, which impacted hundreds of organizations in the United States. Further, the VOHO campaign itself was just one campaign of many that is attributable to this incredibly prolific group. Each campaign is designed to access information in governmental and commercial organizations that tend to operate in the wealthiest and most technologically advanced countries in the world.

Who are the Hidden Lynx group?

The Hidden Lynx group has been in operation since at least 2009 and is most likely a professional organization that offers a "hackers for hire" service. They have the capability to attack many organizations with concurrently running campaigns. They operate efficiently and move quickly and methodically. Based on these factors, the Hidden Lynx group would need to be a sizeable organization made up of between 50 and 100 individuals.

The members of this group are experts at breaching systems. They engage in a two-pronged strategy of mass exploitation and pay-to-order targeted attacks for intellectual property using two Trojans designed specifically for each purpose:

- Team Moudoor distributes Backdoor.Moudoor, a customized version of "Gh0st RAT", for large-scale campaigns across several industries. The distribution of Moudoor requires a sizeable number of people to both breach targets and retrieve the information from the compromised networks.
- Team Naid distributes Trojan.Naid, the Trojan found during the Bit9 incident, which appears to be reserved for more limited attacks against high value targets. This Trojan was leveraged for a special operation during the VOHO campaign and is probably used by a specific team of highly skilled attackers within the group. This Trojan was also found as part of "Operation Aurora" in 2009.

Much of the attack infrastructure and tools used during these campaigns originate from network infrastructure in China. The Hidden Lynx group makes regular use of zero-day exploits and has the ability to rework and customize exploits quickly. They are methodical in their approach and they display a skillset far in advance of some other attack groups also operating in that region, such as the Comment Crew (also known as APT1). The Hidden Lynx group is an advanced persistent threat that has been in operation for at least four years and is breaking into some of the best-protected organizations in the world. With a zero-day attack already under their belt in 2013, they continue to operate at the leading edge of targeted attacks.

Symantec

WHO ARE THEIR TARGETS?

> “The diverse set of targets from a variety of sectors would indicate that this group is not focused on any one specific task.”

Who are their targets?

Since November 2011, hundreds of organizations worldwide have been targeted by the Hidden Lynx group. These organizations have remained relatively consistent during this time period. The group targets organizations operating in both the commercial sector and within all levels of government. The diverse set of targets from a variety of sectors would indicate that this group is not focused on any one specific task. The group manages concurrent campaigns in attacks that are global in nature.

The Hidden Lynx group has most recently conducted attacks against specific organizations in South Korea and has a long history of attacking the defense industrial sector of Western countries.

The top 10 organizations categorized by the verticals they belong to are shown in Figure 1.

The most targeted countries/regions are shown in Figure 2.

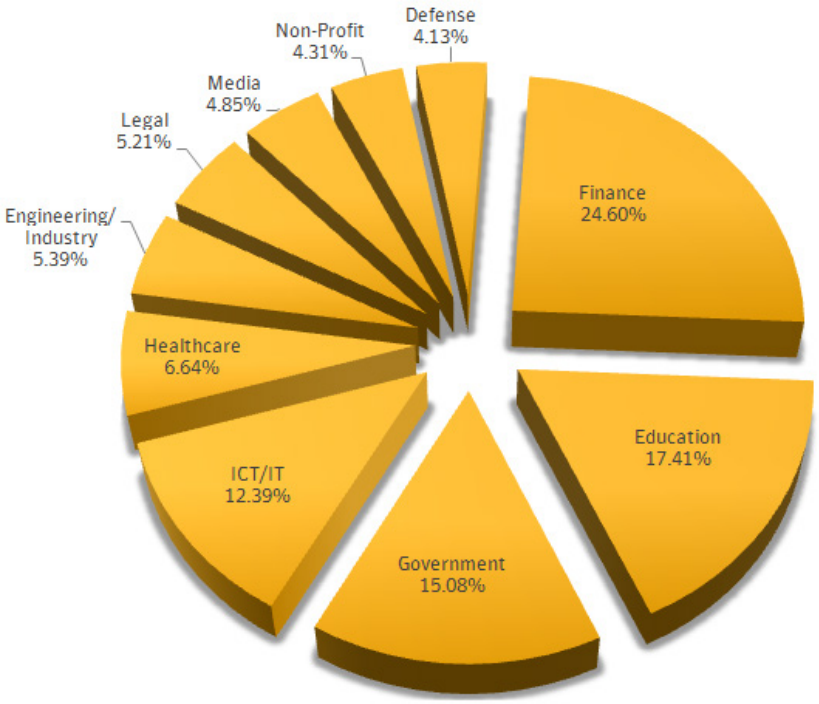


Figure 1. Top 10 organizations targeted by the Hidden Lynx group since November 2011

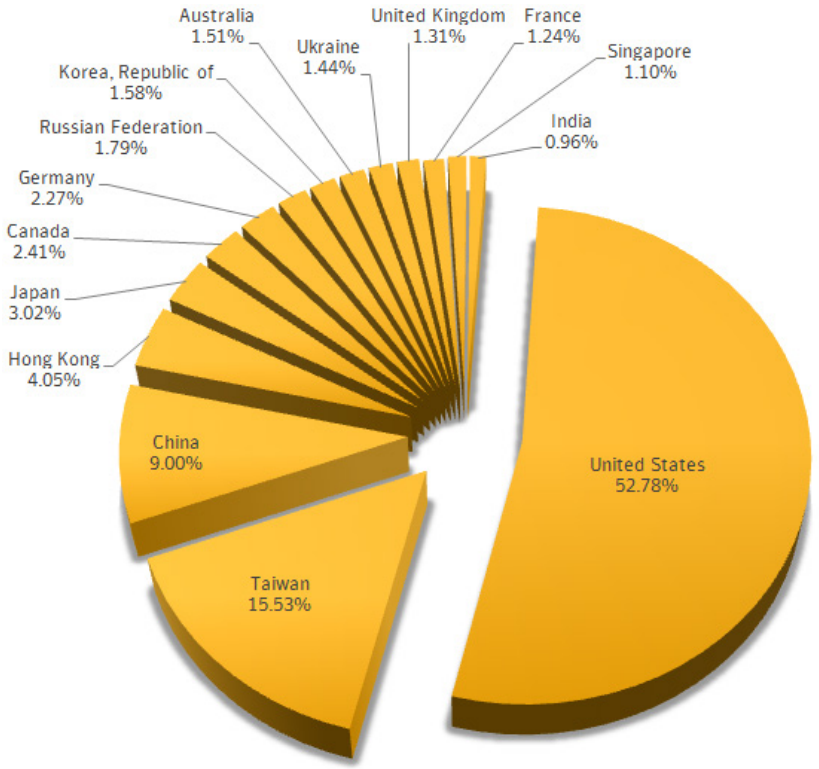


Figure 2. Countries/regions targeted by the Hidden Lynx group since November 2011

What is their motivation?

This broad range of targeted information would indicate that the attackers are part of a professional organization. They are likely tasked with obtaining very specific information that could be used to gain competitive advantages at both a corporate and nation state level. It is unlikely that this organization engages in processing or using the stolen information for direct financial gain. Their mode of operation would suggest that they may be a private organization of “hackers for hire”, who are highly skilled, experienced professionals whose services are available for those willing to pay.

Corporate Espionage

The financial services sector has been identified as the most heavily targeted industry overall. There is a tendency to target specific companies within this sector. Investment banks and asset management agencies account for the majority of organizations targeted within this industry. The absence of certain types of financial institutions, such as those operating as commercial banks, clearly indicates that the attacks are focusing on specific areas. The organizations involved would have expertise in large corporate deals, such as confidential information on upcoming mergers and acquisitions, which could be used to gain a competitive edge. Targeting this sector in such a concentrated fashion could provide invaluable information when negotiating large takeovers or trading shares on the stock exchange.

Attacks on the financial sector are not limited to investment banks. Stock trading firms and one of the world's largest stock exchanges have been subjected to attacks from this group. The Hidden Lynx group has also undertaken indirect attacks through the supply chains. Organizations that supply hardware, secure network communications and services specific to the financial sector have also come under attack. There is almost certainly a financial motivation behind these attacks.

Attacks against government contractors

In attacks that have targeted all levels of government from local to national level, this group has repeatedly attempted to infiltrate these networks. Attacks against government contractors and, more specifically, the defense industry indicate that the group is in pursuit of confidential information and suggests that the group had been working for nation states.

Targeting advanced technologies in specific areas such as aerospace would be useful in order to close technological gaps or gain knowledge of the advanced capabilities of other nation states. Attacks on organizations that operate in the Internet services space can provide a wealth of valuable information. The group had affiliations to "Operation Aurora" (See appendix for more details), a campaign that targeted a number of organizations including software manufacturers and defense contractors. More recently, Microsoft claimed that the target was databases containing emails marked for court order wiretaps. They believe that these attacks were counter-intelligence operations, activities that would provide benefits at a nation state level.

What are they capable of?

The group's tools, tactics and procedures are innovative and typically cutting-edge. They use custom tools and techniques that they tailor to meet their objectives and maximize their chance of success. They attack public-facing infrastructure and have been observed installing highly customized Trojans that are purpose-built for stealth. They engineered one of the most successful watering-hole attacks to-date. They also undertake spear-phishing attacks and hack supply chains in order to distribute their custom Trojans. This is an established team with years of experience. They are well resourced and highly skilled.

The Hidden Lynx group's advanced capabilities are clearly demonstrated in three major campaigns. In the VOHO campaign, they showed how they could subvert Bit9's established trust models. In the FINSHO campaign, they managed to get advanced knowledge of a zero-day exploit and in the SCADEF operation, they undertook supply chain attacks to succeed in their campaign.

Subverting trust protection models

The team can adapt rapidly to counter-measures that would otherwise hinder the success of a campaign. The attack on Bit9 showed how the group could bypass solid trust protection models to get to their targets. However, this attack was only a small part of the larger VOHO campaign, where the group proved how quickly they can adapt and change their tactics in the face of new and unforeseen obstacles.

The Bit9 incident

Bit9 is a security company headquartered in Waltham, Massachusetts. As an alternative to traditional signature-based antivirus solutions, Bit9 offers a trust-based security platform that runs off of a cloud-based reputation service combined with policy-driven application control and whitelisting to protect against cyberthreats. As a result, it is difficult for a malicious third-party to install an untrusted application, such as a remote access Trojan (RAT), onto a system that is adequately protected with the Bit9 platform. Undaunted by this, the elite Hidden Lynx group took up the challenge.

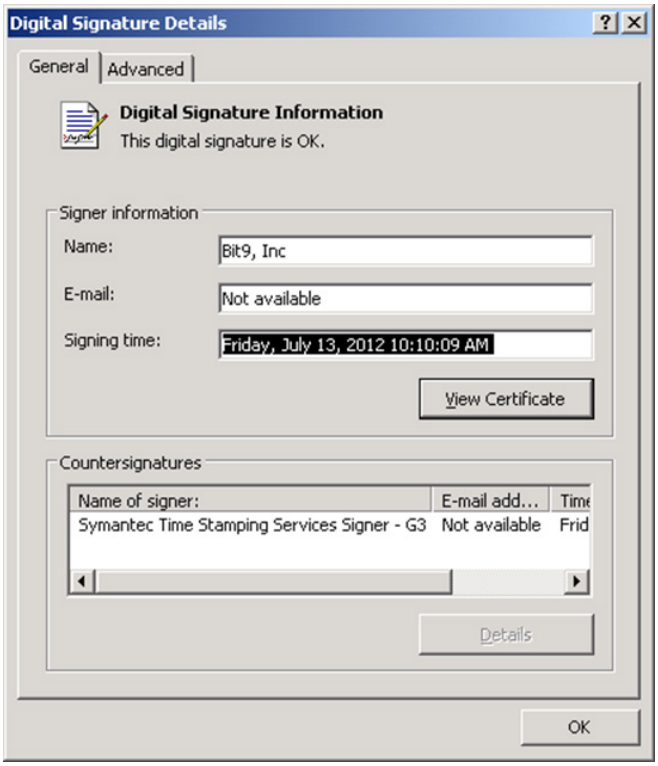


Figure 3. Trojan.Naid – Bit9 digital certific ate, July 13, 2012, provided by Symantec's CA

On February 8 2013, Bit9 released details revealing that a malicious third-party had gained access to one of their digital code-signing certificates. During this incident, a number of Trojans and malicious scripts were signed. In a follow up post on February 25, more details of the attack emerged. In July 2012, more than six months earlier, a malicious third-party gained access to their network using an SQL injection attack. Due to an operational oversight, a public-facing server that wasn't protected with the Bit9 platform allowed the attackers to gain unauthorized access.

The attackers installed Backdoor.Hikit, a Trojan that provides extremely stealthy remote access to compromised systems. This highly customized Trojan is typically installed onto servers in the victims' DMZ, which was the case at Bit9. Credentials for another virtual machine were then stolen. These were used to access the virtual machine that contained one of Bit9's digital code-signing certificates. The attackers used this code-signing infrastructure to sign thirty-two malicious files. Symantec telemetry shows some of these files have been present within select organizations in the United States defense industrial sector.

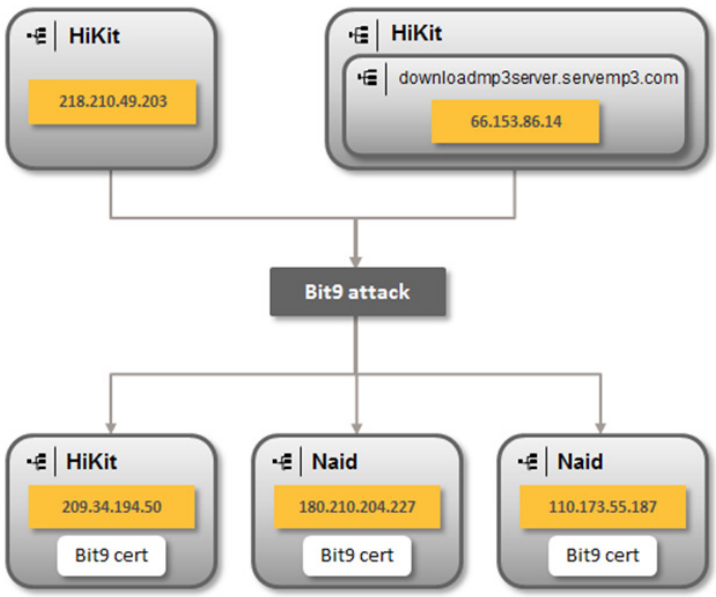


Figure 4. Trojans successfully acquired with command-and-control (C&C) servers from the Bit9 investigation

The signing of these files is significant, since they could then be used to circumvent the trust protection model offered by the Bit9 platform. The Trojans signed include variants of Backdoor.Hikit (the remote access Trojan used in the initial compromise) and another RAT called Trojan.Naid. Some malicious attack scripts were also signed. Each Trojan has a specific purpose. Backdoor.Hikit was used to target public-facing infrastructure while Trojan. Naid was used to perform highly targeted attacks through email and watering-holes.

Bit9 was alerted to the compromise in January 2013 and took immediate containment steps such as revoking the digital signature and reaching out to their entire customer base. According to Bit9, the attacks that followed

were not financially motivated, but rather were an attempt to access information. On Bit9's own admission, three customers were impacted.

In conjunction with the Bit9 compromise, the Hidden Lynx group had another significant campaign well under way. They had just concluded phase one of the VOHO campaign, a watering-hole operation orchestrated to attack organizations in the Boston, Massachusetts area – it was a likely a distribution vector for the newly signed files.

The VOHO campaign

The VOHO campaign, first publicized by RSA, is one of the largest and most successful watering-hole attacks to date. The campaign combined both regional and industry-specific attacks and predominantly targeted organizations that operate in the United States. In a rapidly spreading two-phase attack, which started on June 25 and finished July 18, nearly 4,000 machines had downloaded a malicious payload. These payloads were being delivered to unsuspecting victims from legitimate websites that were strategically compromised.

Figure 5. The VOHO campaign target regions and industries

This watering-hole infection technique was quite innovative at the time. In a watering-hole attack, the attacker compromises a legitimate website that the target uses and trusts. The attacker then lies in wait for the target to visit the compromised site in order to infect them. The scale and targeted nature of the VOHO campaign set it apart from watering-hole attacks observed in the past. The group first adopted this technique in December 2011 when an exploit for the Oracle Java SE Rhino Script Engine Remote Code Execution Vulnerability (CVE-2011-3544) was leveraged to distribute their payloads. As a result of their success, many other strategic compromises have been adopted by other attack groups, as seen in a notable attack targeting iOS developers earlier in 2013 which impacted employees at Facebook, Apple and Twitter.

In the VOHO campaign, ten legitimate websites were strategically compromised. The attackers carefully selected these websites based on the likelihood that the intended target(s) would visit them during the exploit delivery phase. The attackers likely pre-determined who visited the watering-hole in advance of the distribution phase of attack. This could easily be achieved by examining the access logs of compromised Web servers. The categories of websites compromised were both regional and industry-specific in nature and targeted the following key areas illustrated in Figure 5.

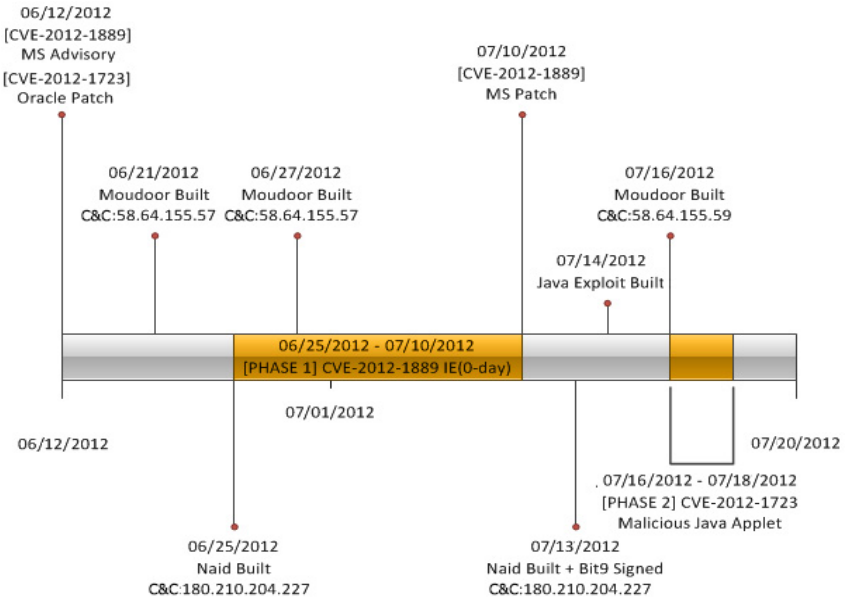


Figure 6. The VOHO campaign malicious activity timeline - a two-phase attack

Timeline of activity

The VOHO watering-hole distributed remote access Trojans in two phases. In phase one of the attack, an Internet Explorer zero-day vulnerability, the Microsoft XML Core Services CVE-2012-1889 Remote Code Execution Vulnerability (CVE-2012-1889), was leveraged. On July 10, Microsoft introduced the patch for CVE-2012-1889 and activity at the watering-hole ceased. This appears to have been a clever decision on behalf of the attackers. If they continued to deliver the exploit, they risked detection and would have hurt their chances of retaining access to the watering-hole for phase two of the campaign. Within six days, phase two of the distribution began, this time using a malicious Java applet exploiting the Oracle Java SE CVE-2012-1723 Remote Code Execution Vulnerability (CVE-2012-1723). This Java exploit was patched at the time. Having already used two zero-day exploits in quick succession (the first zero-day exploit was used in the GOTHAM campaign in May 2012, see appendix for more details), the Hidden Lynx group may not have had another one at their disposal.

The timeline of activity at the watering-hole is shown in Figure 6.

In each phase of the attack, two Trojans were being distributed at different intervals. The customized version of "Gh0st RAT", Backdoor.Moudoor, saw large-scale distribution in comparison to Trojan.Naid, which was used more selectively in these attacks.

Before being used in the second phase of the attack, Trojan.Naid was signed with the Bit9 certificate. Moudoor was never observed during the attack on Bit9, which could indicate that two separate teams are at work here. With Moudoor and Naid using different command-and-control (C&C) servers, each team could work independently on alternative objectives. The discovery of the Naid C&C would also be less likely in comparison to Moudoor's, as its large-scale distribution would inevitably create more noise as it continued to impact many organizations.

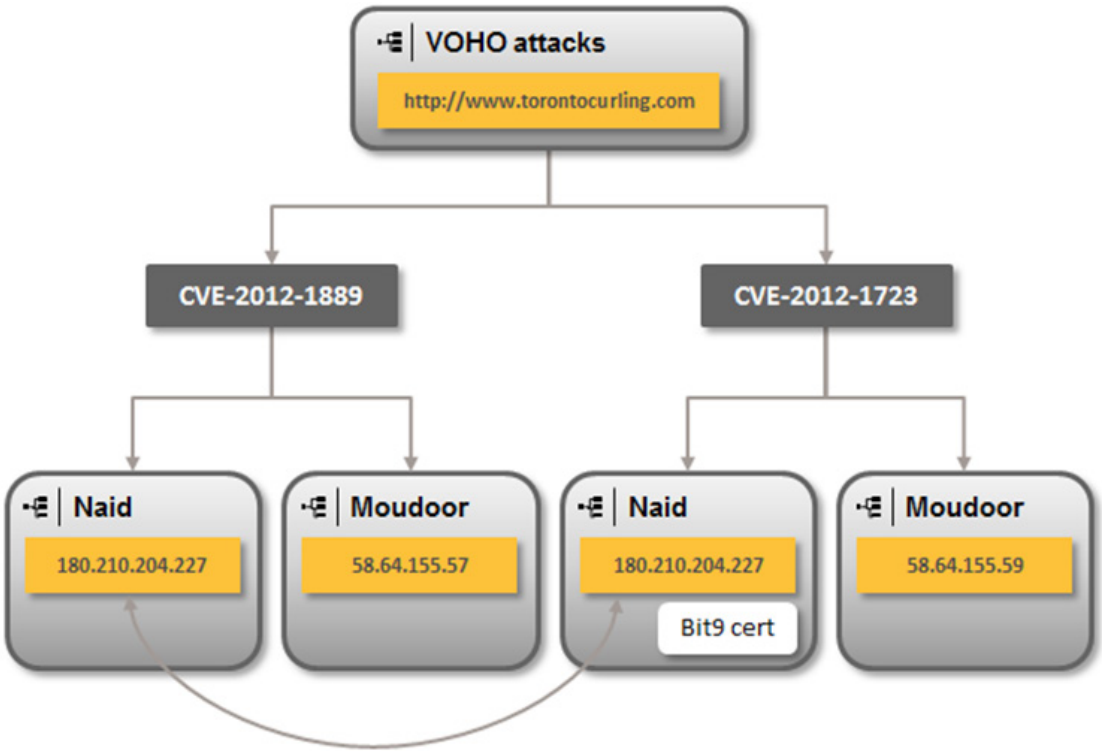


Figure 7. The VOHO campaign – Trojans distributed and C&C servers used to command and control

Team Naid's role

During this campaign, Team Naid had a very specific objective – to gain access to information from organizations operating in the defense industrial sector. An unsigned version of Naid was distributed to select victims within the defense industrial sector during phase one until Microsoft supplied a patch for CVE-2012-1889 on July 10. It may have been during this phase of the attack when the team realized the information they sought was held by organizations protected by Bit9. As the team found it difficult to compromise Bit9-protected computers and had no viable exploit for distribution, their immediate objective focused on Bit9's digital code-signing certificate.

By July 13, just a few days after they started their attacks on Bit9, they obtained the Bit9-signed Naid. By the next day, they had built a viable Java exploit to distribute their Trojan. Armed with the newly-signed Trojan and delivery vehicle, the group resumed malicious activity at the watering-hole for three days from July 16. It was during this period that three organizations protected with the Bit9 platform were successfully compromised.

In this campaign, Naid was specifically reserved for special operations against high value targets. Team Naid's objective was narrow and focused and the team aimed to limit Naid's exposure. The sophistication of the overall attack is typical of attackers with a very high pedigree. The team is clearly highly skilled; they operate methodically and can switch objectives at a moment's notice. They rapidly adapted to external factors that were hindering their specific objective and pursued a difficult prize - the Bit9 certificate - in order to achieve their overall goal.

Team Moudoor's role

The distribution of Moudoor during this campaign was on a much larger scale. Organizations operating in the financial sector, all levels of government (local and federal), healthcare, education and law were impacted during this campaign. There is a wealth of sensitive information within these organizations which would be of interest to both nation states and entities that would benefit from information as a result of corporate espionage attacks.

The top distinct infections per organization type are shown in Figure 8.

A campaign distributing Moudoor on such a large scale would require a sizeable team to operate and maintain remote access to these compromised computers. The breach phase of the operation could easily be handled by a smaller team, which then passes control to a larger team of operators who can traverse networks and retrieve the information they are tasked with gaining access to. To efficiently

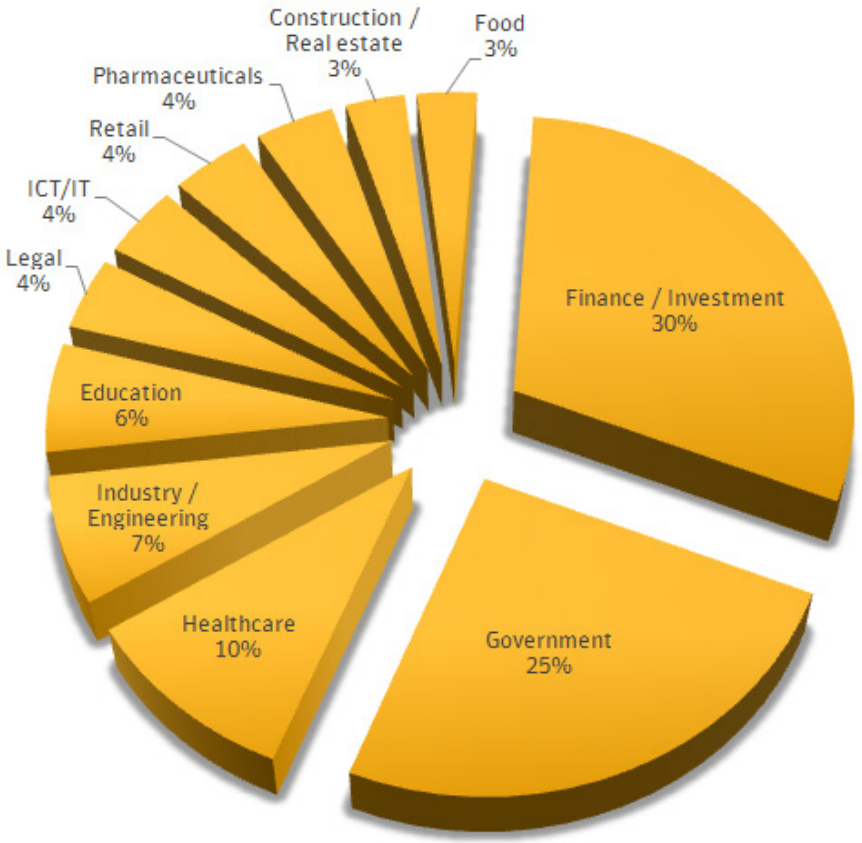


Figure 8. Industries with the most Backdoor.Moudoor infections during the VOHO campaign

attack this many organizations concurrently would require an equally large number of operators. These Trojans require manual operation so it's conceivable that tens if not hundreds of operators would be used post-breach to process and handle the stolen data.

The VOHO campaign is one of a number of campaigns attributed to this group over the last four years. It showed how quickly the group could change their strategy and the lengths they would go to get to their targets. The fact that the Bit9 code-signing certificate breach was only a small part of this campaign shows how adaptable and determined the group is.

Advanced zero-day access

The group is highly organized and can gain advanced access to zero-day vulnerabilities. In February, the Hidden Lynx group used this advanced knowledge to take advantage of the Oracle Java SE CVE-2013-1493 Remote Code Execution Vulnerability (CVE-2013-1493) to attack Japanese targets in the FINSHO campaign.

FINSHO

Within two days of Bit9's blog post on February 25, the attackers began distributing Moudoor and Naid in a campaign that leveraged CVE-2013-1493. Interestingly, the C&C server configured in Naid (110.173.55.187) was also configured in a sample found in the Bit9 incident. Although the version used against Bit9 was not observed elsewhere in the wild, the group's methodical approach would indicate that a similar campaign may have been intended for that Trojan.

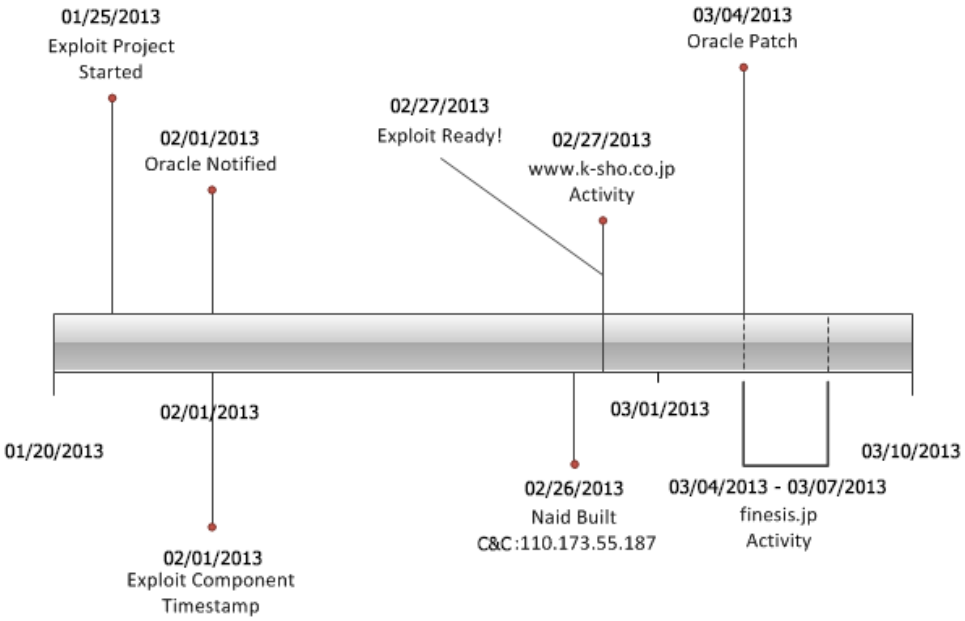


Figure 9. Timeline of activity for CVE-2013-1493 distributing Moudoor and Naid in the FINSHO campaign

The timeline for exploit development and distribution is illustrated in Figure 9.

According to Oracle's blog, CVE-2013-1493 was reported to them on February 1, the same day that class files exploiting it were added to MightDev.jar shown in Figure 10. In past Java exploits used by this group, the code was already public knowledge and a patch was already available for the software. In this case, they gained advanced knowledge from an unknown source - a source with early access to the exploit conditions, possibly on the same day as Oracle. Oracle released the fix for CVE-2013-1493 on March 4.

Name	Ext	Size	Date	Attr
[META-INF]		<DIR>	02/27/2013 13:43	---
.classpath		301	01/25/2013 15:37	---
.project		383	01/25/2013 15:37	---
ImAlpha	class	7,248	02/27/2013 13:40	---
ImAlpha$Leak	class	546	02/01/2013 14:39	---
ImAlpha$MyBufferedImage	class	1,732	02/01/2013 14:39	---
ImAlpha$MyColorSpace	class	852	02/01/2013 14:39	---

Figure 10. MightDev.jar used to distribute Naid and subsequently Moudoor

Figure 11 illustrates the relationship between FINSHO and the Bit9 incident through the shared C&C server used in both Naid configurations.

Alternate C&C servers and separate websites for distribution provide further evidence that there are distinctions between how these teams operate.

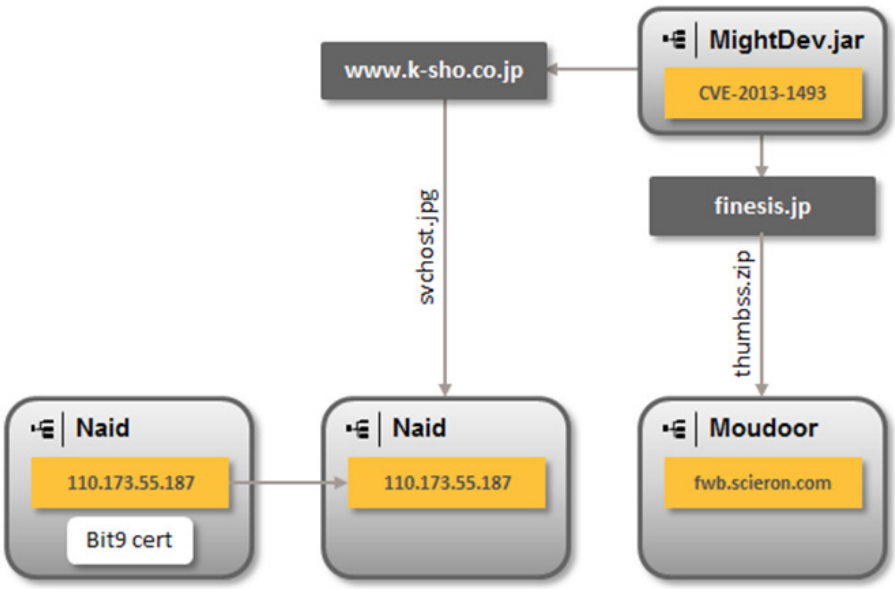


Figure 11. CVE-2013-1493 used to distribute Trojan.Naid and Backdoor.Moudoor (February/March 2013) in the FINSHO campaign

Supply chain attacks

The Hidden Lynx group continued to attack the defense industry post-VOHO. In another campaign named SCADEF, manufacturers and suppliers of military-grade computers were observed installing a Trojanized Intel driver application.

SCADEF

The attackers bundled this Intel driver application with variants of Backdoor.Moudoor using a popular Chinese archiving application called Haozip. The attackers likely compromised a legitimate download of this driver application from a non-reputable source but the true source was never discovered in this investigation.

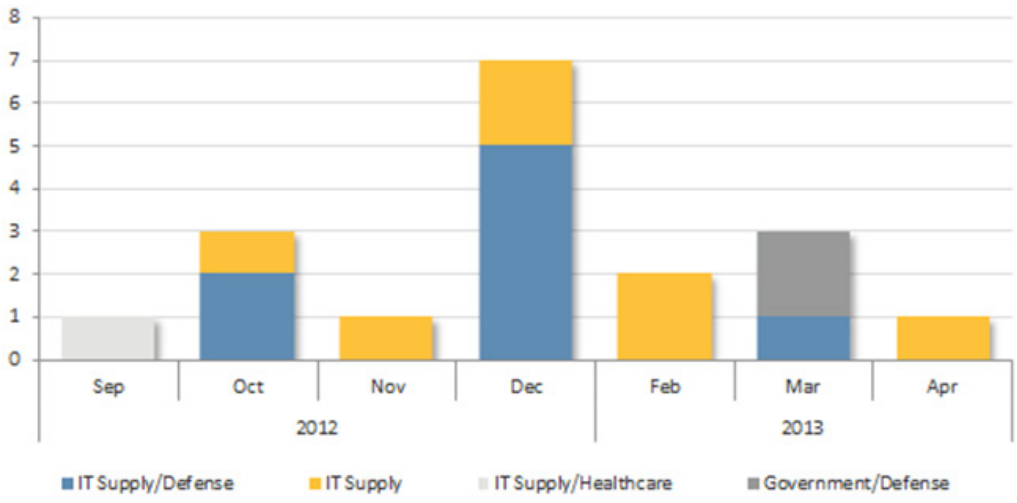


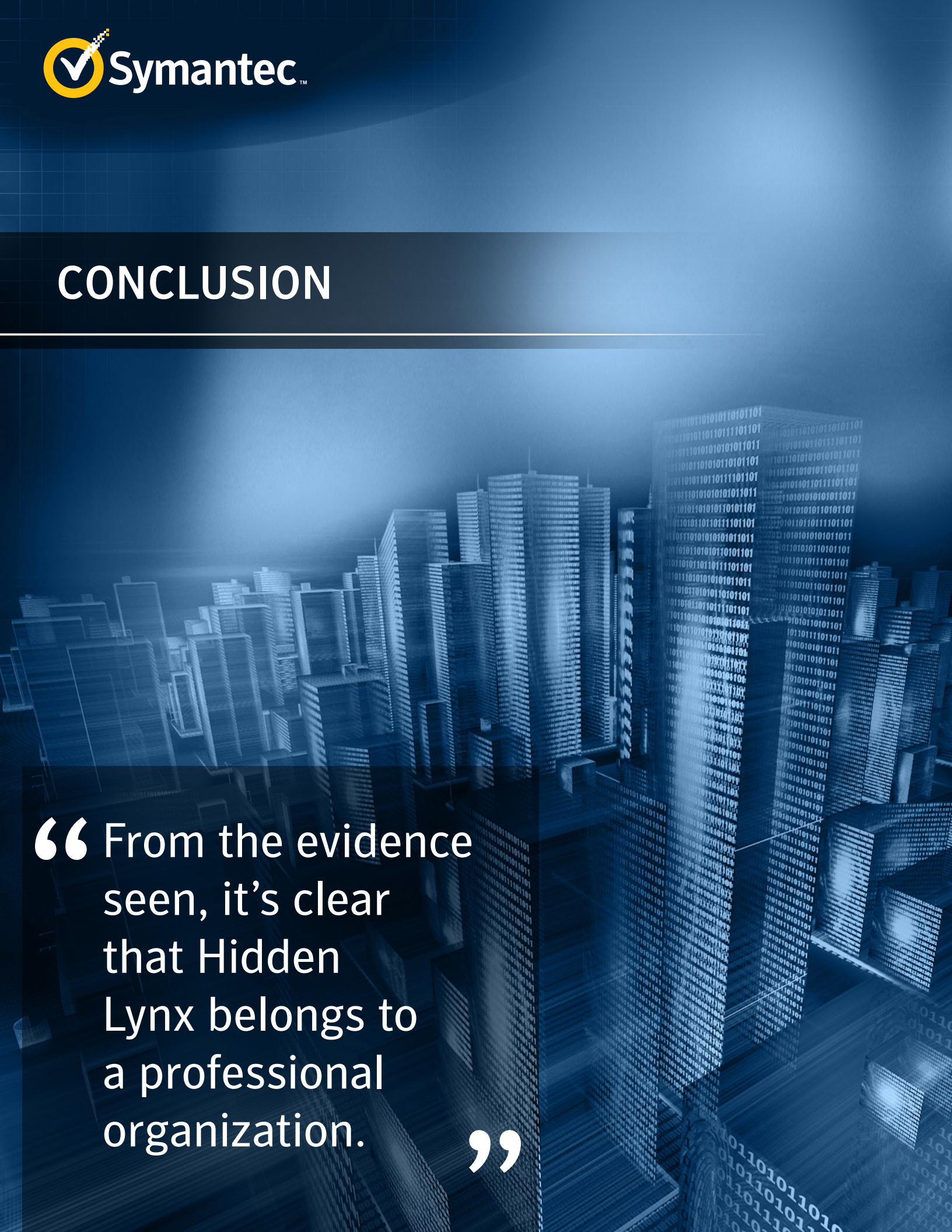
Figure 12. Supply chain hacking detections in the IT supply/defense/healthcare industry

The technique is another avenue into hardened networks of interest. They attack not only hardware suppliers, but contractors that may access these networks during their course of work. The group seeks out the weakest link in the chain and simply lies in wait. In these specific attacks, they simply wait for a shipment of compromised computers to be installed into the targeted network. Unique detections observed for these Trojanized applications are presented in Figure 12.

The VOHO, FINSHO and SCADEF campaigns each showed how efficient and adaptable the group is when focusing on their targets. They use a wide range of advanced attack methods and change their strategy when required to carry out each operation. These three campaigns are only some of the operations undertaken by the Hidden Lynx group, making them a credible threat to several industries.

Symantec

CONCLUSION



> “From the evidence seen, it’s clear that Hidden Lynx belongs to a professional organization.”

Conclusion

Cyberespionage campaigns are becoming increasingly common, with countless threat actors attempting to gain footholds into some of the best-protected organizations. These attacks are becoming increasingly sophisticated. The capabilities and tactics used by these threat actors vary considerably. The Hidden Lynx group is capable of undertaking focused attacks against niche targets and running large-scale campaigns targeting multiple organizations on a global scale. They have seen action in numerous campaigns since 2009 and repeatedly attack their targets with cutting-edge techniques. They quickly adapt to security counter-measures and are highly motivated. They are one of the most well-resourced and capable attack groups in the targeted threat landscape.

From the evidence seen, it's clear that Hidden Lynx belongs to a professional organization. They operate in a highly efficient manner. They can attack on multiple fronts. They use the latest techniques, have access to a diverse set of exploits and have highly customized tools to compromise target networks. Their attacks, carried out with such precision on a regular basis over long periods of time, would require a well-resourced and sizeable organization. They possess expertise in many areas, with teams of highly skilled individuals who can adapt rapidly to the changing landscape. This team could easily consist of 50-100 individuals. This level of resources would be needed to build these Trojans, maintain infection and C&C infrastructure and pursue confidential information on multiple networks. They are highly skilled and experienced campaigners in pursuit of information of value to both commercial and governmental organizations.

The incident in Bit9, which ultimately led to successful compromises of hard-to-crack targets during the VOHO campaign, only serves to highlight this fact. The evolving targeted attack landscape is becoming increasingly sophisticated. As organizations implement security counter-measures, the attackers are adapting at a rapid rate. With a growing number of threat actors participating in these campaigns, organizations have to understand that sophisticated attackers are working hard to bypass each layer of security. It's no longer safe to assume that any one solution will protect a company's assets. A variety of solutions need to be combined and, with a better understanding of the adversary, tailored to adequately protect the information of most interest to the attackers.

The Hidden Lynx group's mission is large and they're targeting a diverse set of information. The frequency and diversity of these attacks would indicate that the attackers are tasked with sourcing information from many organizations. These tasks are likely distributed within the team. The group's goal is to gain access to information within organizations in some of the wealthiest and most technologically advanced countries across the globe. It is unlikely that they can use this information for direct financial gain, and the diversity of the information and number of distinguishable campaigns would suggest that they are contracted by multiple clients. This leads us to believe that this is a professional organization that offers a "hackers for hire" service.

The worrying knock-on effect of this group's activities is that other threat actors are learning and adopting their techniques. The Hidden Lynx group is not basking in their past glories, they are continuing to refine and streamline their operations and techniques to stay one step ahead of their competition. Organizations that are being attacked on multiple fronts need to better protect the information that is most valuable to them. We expect these attackers to be involved in many more high profile campaigns in the coming years. They will continue to adapt and innovate. They will continue to provide information servicing interests at both a corporate and state level. Groups like Hidden Lynx are certainly winning some of the battles, but as organizations gain a better understanding of how these groups operate, they can take steps to help prevent their most valuable information from falling into attackers' hands.

APPENDIX

Appendix

Related attacks

The three campaigns that have already been examined in detail are only a snapshot of the group's activities. Since the time they adopted Moudoor in late 2011, persistent attacks against organizations across the globe have been occurring on a regular basis, even to this day. These attackers pioneered the watering-hole technique, however they can also fall back to more traditional methods of attack, such as spear-phishing emails, supply chain attacks and Trojanized software updates. Since 2011, the Hidden Lynx group has leveraged five browser-based exploits for payload distribution, three of which were zero-day exploits.

Table 1. Vulnerabilities associated with Naid/Moudoor distribution (Nov 2011 – March 2013)

CVE	Description	Exploit Website
CVE-2011-3544	Oracle Java Rhino Script Engine	http://www.wsdhealthy.com http://www.tade.org.tw http://www.gnnet.co.kr
CVE-2012-1875	Microsoft Internet Explorer - Same ID Property RCE Vulnerability	http://www.gothamcenter.org http://www.villagemania.it
CVE-2012-1889	Microsoft XML Core Services CVE-2012-1889 RCE Vulnerability	http://www.gothamcenter.org http://www.torontocurling.com (VOHO) http://ansky.hk166.cqbi.com
CVE-2012-1723	Oracle Java SE CVE-2012-1723 RCE Vulnerability	http://www.torontocurling.com (VOHO)
CVE-2013-1493	Oracle Java SE RCE Vulnerability	http://www.k-sho.co.jp http://www.finesis.jp

The list of browser-based exploits used by the Hidden Lynx group since the introduction of Moudoor is presented in Table 1.

In the first half of 2012, there was a particularly high distribution of Moudoor. There was a peak in June/July as a result of the VOHO campaign which is evident in the graph shown in Figure 13.

There is also a peak at the beginning of the year which is a result of another high distribution campaign called WSDHEALTHY. This campaign, along with some other notable attacks and techniques, will be discussed in the following sections.

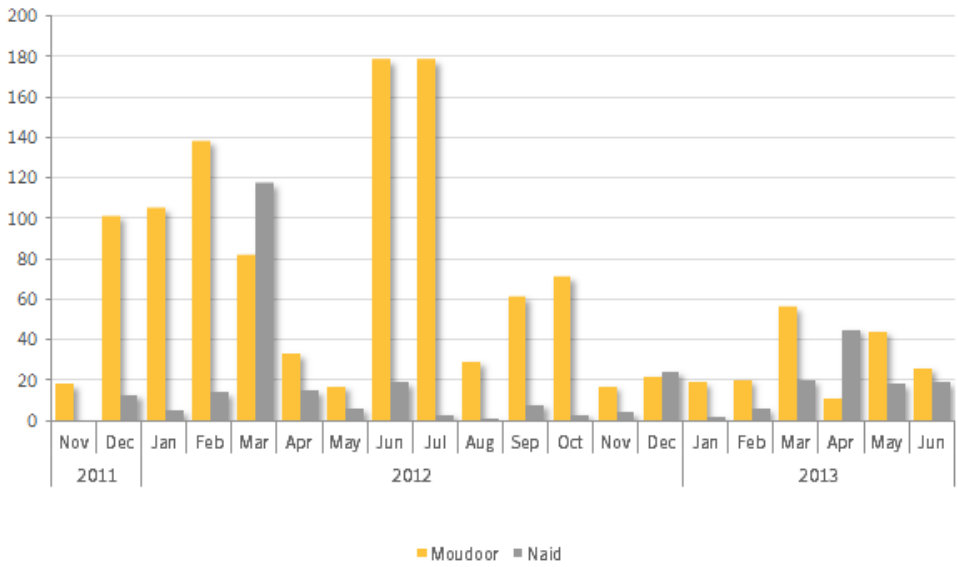


Figure 13. Unique infections of Moudoor and Naid (November 2011 – June 2013)

- GOTHAM – Shared distribution, shared C&C – yet another zero day exploit
- WSDHEALTHY – Watering-hole campaigns pre-dating VOHO by seven months
- EASYUPDATE – Trojanizing a popular P2P software's updates

GOTHAM – Campaigns running concurrently

On May 30th, The Hidden Lynx group used their first zero-day exploit of 2012, taking advantage of the Microsoft Internet Explorer CVE-2012-1875 Same ID Property Remote Code Execution Vulnerability (CVE-2012-1875) in order to distribute Moudoor and Naid from gothamcenter.org, a website devoted to the history of New York. This was a two-phase attack which saw Team Naid and Team Moudoor share C&C infrastructure (219.90.117.132) in a smaller campaign that infected organizations in the following industries:

- Financial services
- Information communications technology
- Government
- Marketing
- Information technology
- Aerospace/defense
- Energy

Many of the industries targeted in this campaign are similar to those targeted in the VOHO campaign, so this could be considered as a pre-cursor to that campaign. Similar to VOHO, this was a two-phased attack that leveraged two Internet Explorer zero-days for distribution (CVE-2012-1875 and CVE-2012-1889). Similar to VOHO, as Microsoft patched CVE-2012-1875, the attackers halted distribution. This prevented any unnecessary suspicious activity from being identified that could impact future activity from the compromised website. A timeline for this activity is presented in Figure 14.

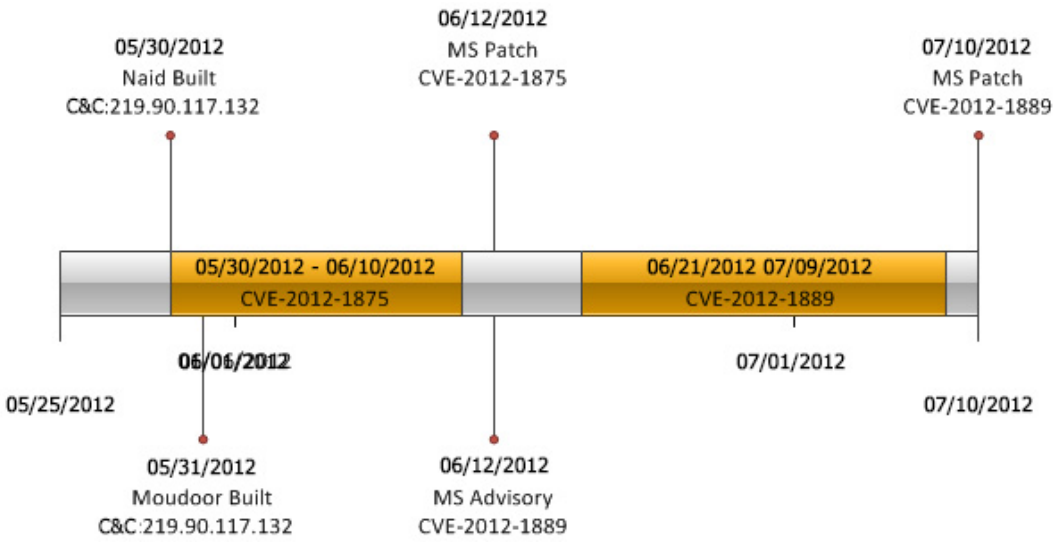


Figure 14. Activity timeline on gothamcenter.org

Sharing C&C infrastructure could indicate that both teams were working closely together and may have divided up the effort during this campaign. During phase two of this campaign, VOHO began. The Hidden Lynx group is clearly resourced to operate and maintain distribution and C&C infrastructure across multiple campaigns. This level of organization requires discipline at multiple levels within the group. This is not a small group of elite hackers – this is a well-organized professional organization.

One campaign that rivals VOHO in terms of size is WSDHEALTHY. This is the first campaign where we see the group using Naid and Moudoor together sharing infrastructure and the first links to the Bit9 incident

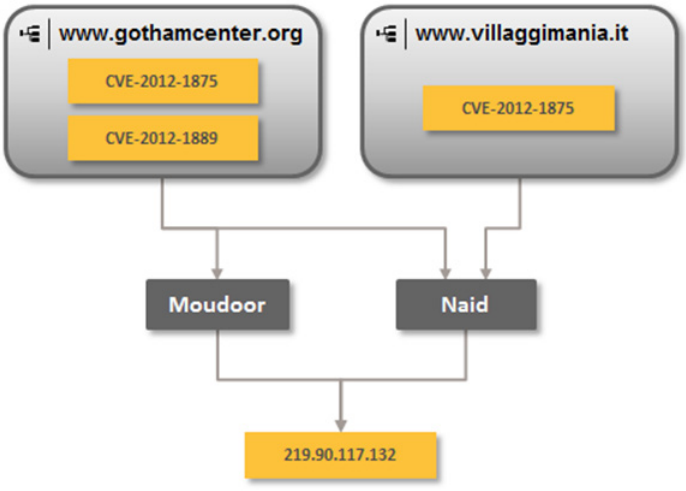


Figure 15. Moudoor and Naid share distribution and command and control servers

start to emerge.

WSDHEALTHY – Shared infrastructure with the Bit9 incident

The Hidden Lynx group began using watering-hole attacks as early as December 2011. Although no zero-day exploit was available, they used a patched Java exploit (CVE-2011-3544) effectively to distribute Moudoor from three compromised websites. This campaign provided the first indications that the group was using both Moudoor and Naid to attack targets and share C&C infrastructure. Along with this, early links to the attacks on Bit9 began to emerge.

The timeline of this activity is shown in Figure 16.

In these campaigns, the Hidden Lynx group made heavy use of infrastructure in Hong Kong, with the exception of yahooeast.net. This is this domain that links to the Bit9 attack, as it resolved to 66.153.86.14 – a C&C server used by the Backdoor.Hikit sample installed after the successful SQL injection attack on Bit9. Moudoor was being actively distributed from these websites for two, four and five months respectively. These are exceptionally long periods of time to retain access to compromised servers for payload distribution of this nature.

The C&C servers used and the links between the Trojans and Bit9 are shown in Figure 17.

Team Moudoor heavily relies on a dynamic DNS service called DTDNS to rapidly switch between C&C servers. In fact, they use direct IP connections or DTDNS exclusively to establish C&C communications, with the

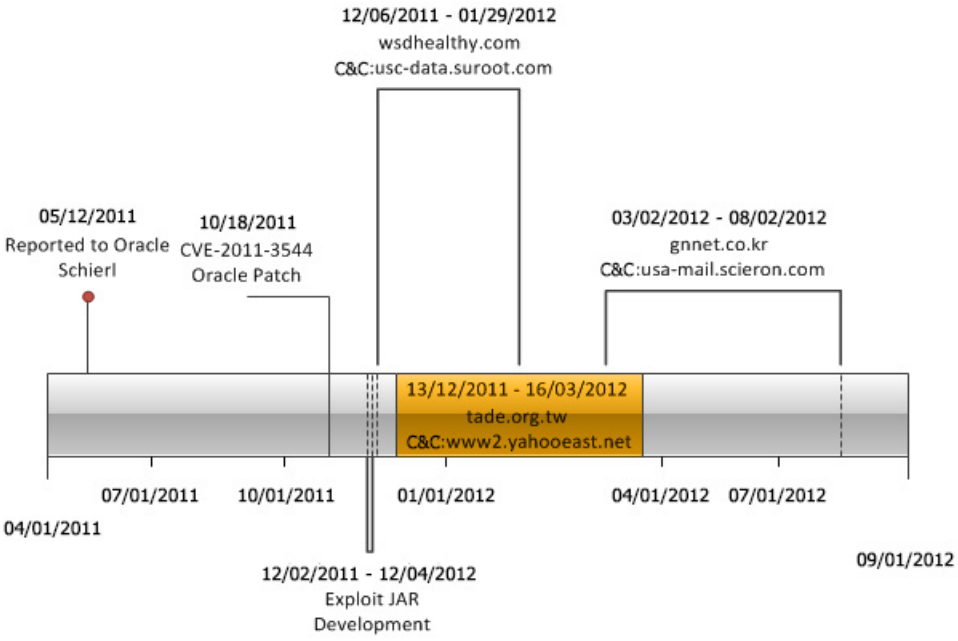


Figure 16. Timeline of malicious activity associated with CVE-2011-3544

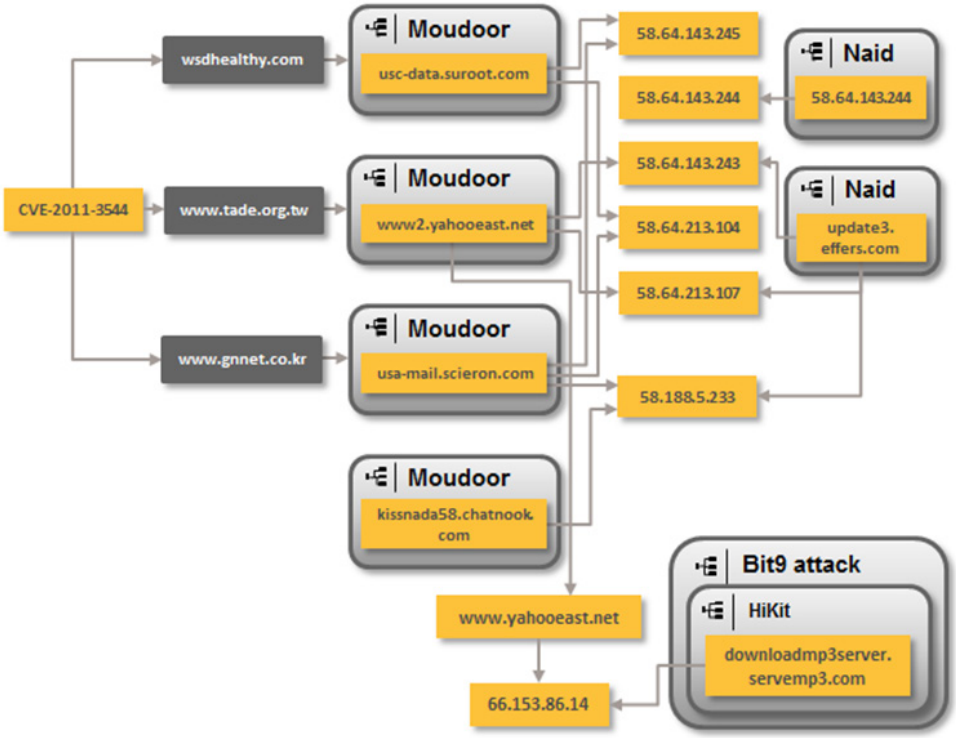


Figure 17. CVE-2011-3544 - the first links between Moudoor and Naid emerge

exception of yahooeast.net which is a registered domain. The Hidden Lynx group uses techniques which have clearly been established through experience to maintain this infrastructure for long periods of time. They adapt quickly and likely have a stockpile of C&C servers that they can quickly switch to which provides maximum uptime during any given operation.

Along with this, the Hidden Lynx group uses several different methods to infect their targets. In the SCADEF campaign, we saw how the group bundled Moudoor with legitimate software to infect targets. They also managed to Trojanize software updates as well, as seen in the EASYUPDATE campaign where a Chinese P2P application was observed selectively installing Moudoor since 2011.

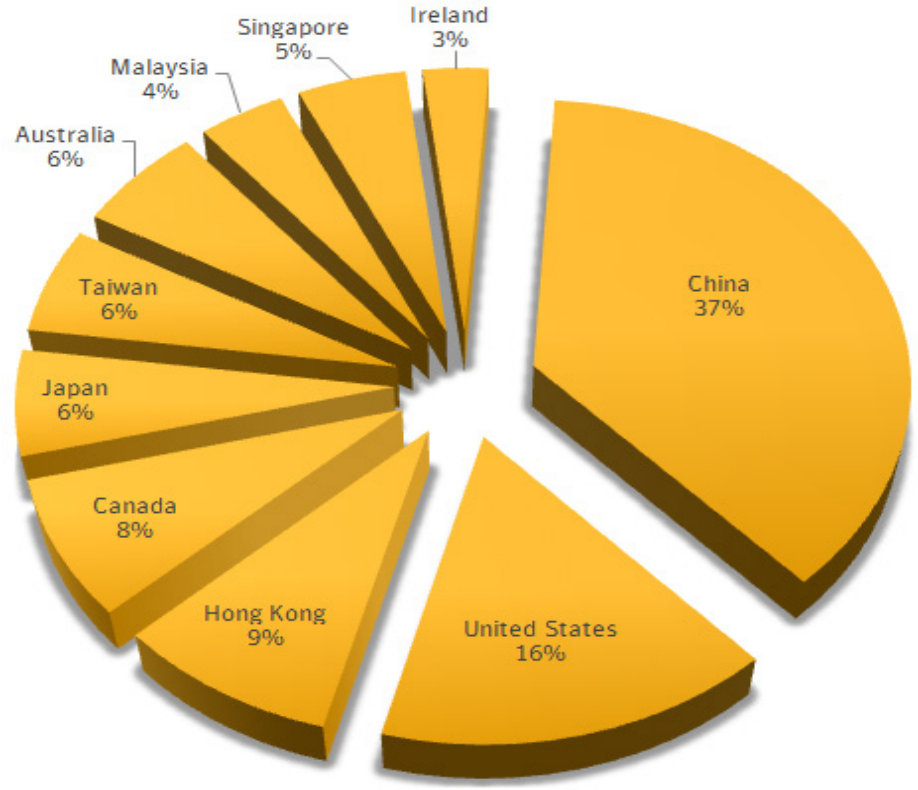


Figure 18. Percentage breakdown of unique detections from VeryCD P2P client

EASYUPDATE – A Trojanized software update

Since November 2011, the Hidden Lynx group has been able to insert Moudoor into the distribution chain of one of the most popular Chinese P2P applications provided by VeryCD.com. There is a very low distribution of Trojanized updates and it is quite likely that they are somehow selectively installing Moudoor on specific clients. This is, without a doubt, the longest running distribution vector for the group, which infected victims predominantly in China, the United States and Hong Kong.

These are the earliest indications of Moudoor infections, with "kissnada" being one of the first DTDNS domains observed in use. This distribution vector's exact purpose is still unclear, however it's certainly linked to the group,

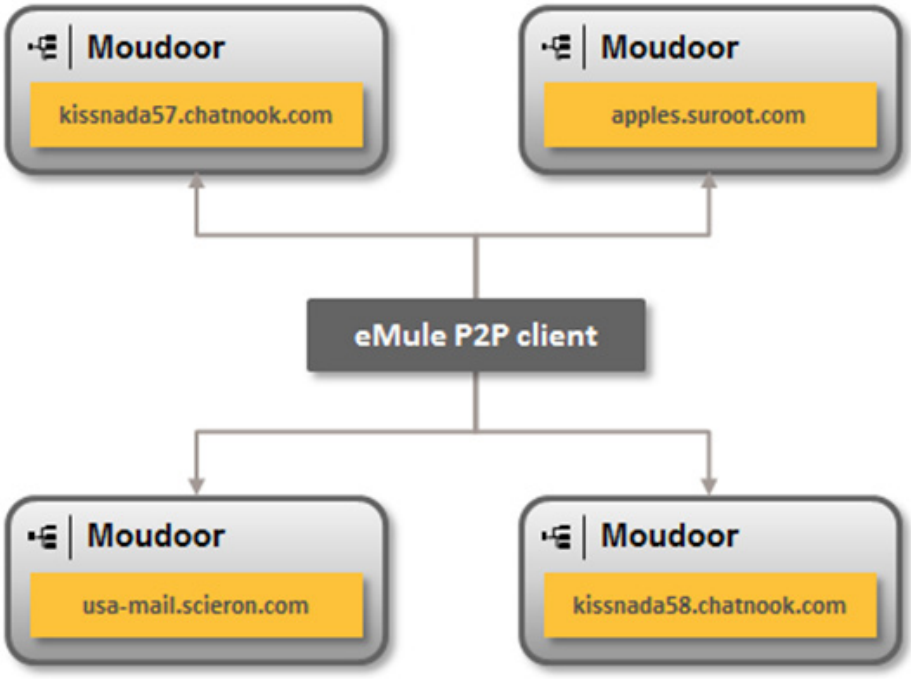


Figure 19. Moudoor variants downloaded through P2P client updates

as we have observed Moudoor samples in WSDHEALTHY configured to use kissnada58.chatnook.com and usa-mail.scieron.com for C&C communications.

The Hidden Lynx group has left a clear fingerprint for the past two years with clearly identifiable links to the group's activities. The use of customized Trojans, shared distribution and C&C infrastructure, coupled with repeated attacks on a predictable set of target organizations has allowed a more complete picture of these attacks to be compiled. A summary of the links between all of these attacks is presented in Figure 20.

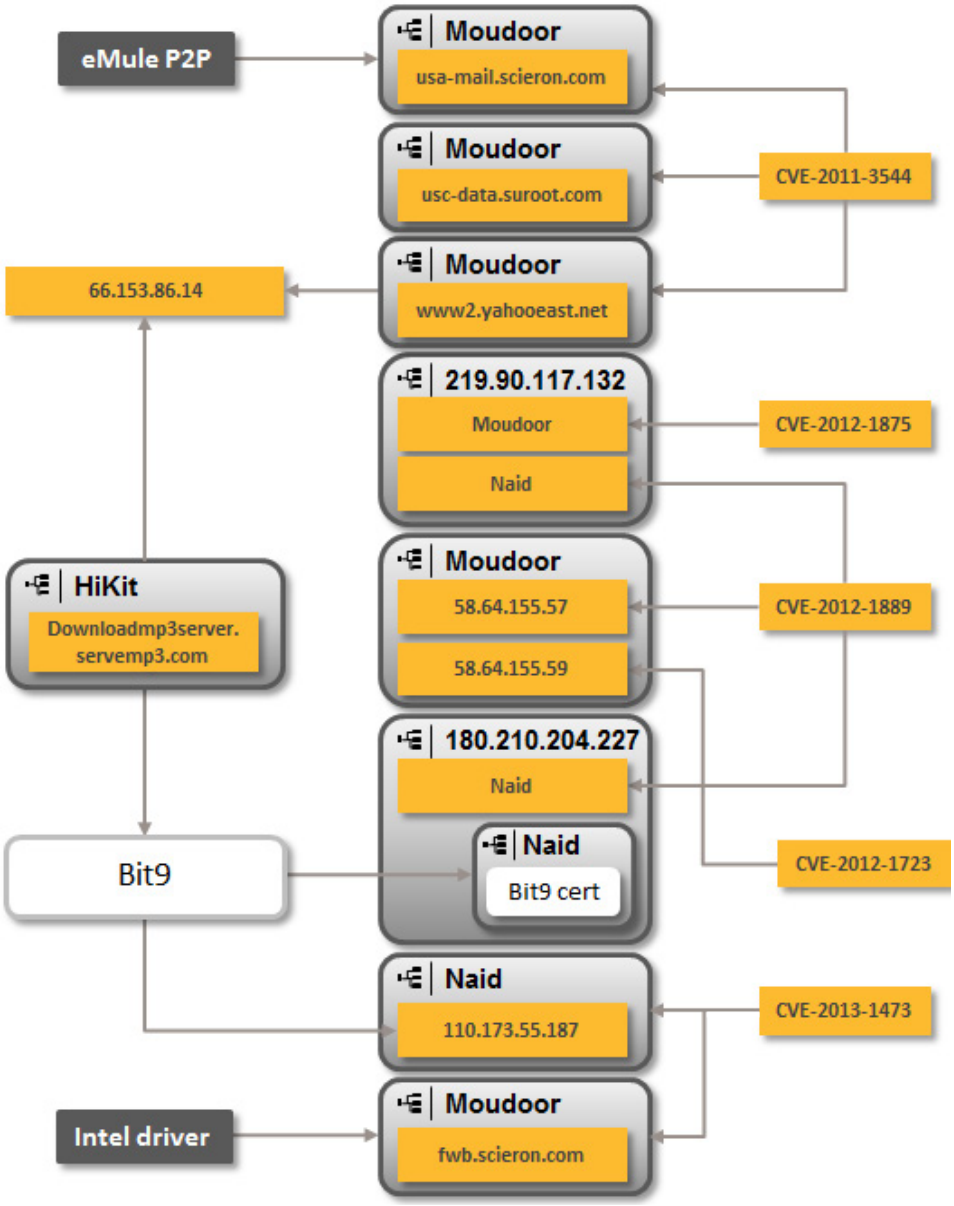


Figure 20. Linking the group's activity (November 2011-March 2013)

Trojans used by the Hidden Lynx group

The following section lists the Trojans that were used by the Hidden Lynx group throughout their various campaigns.

Backdoor.Moudoor

In 2011, the Hidden Lynx group began to use Backdoor.Moudoor. This is a customized version of "Gh0st RAT". Gh0st RAT variants have been used in cyberespionage campaigns emanating from China for years. In 2009, Information Warfare Monitor published a detailed report, "Tracking GhostNet", following an investigation into a cyberespionage network of more than 1,000 compromised computers affecting more than 100 countries. Many threat actors use customized versions of this RAT for cyberespionage operations.

Figure 21. Naid/Vasport obfuscation tool

Trojan.Naid

The team uses Trojan.Naid for special operations. It first appeared in May 2009 and has been used in many high profile attacks over the past four years. It shares

technical similarities with other Trojans which also originate from China. All of these Trojans are potentially from the same group or they may source these Trojans from the same developer. The technical similarities are based on a shared file creation template and C&C protocol.

The other Trojans that share these traits are:

- Backdoor.Vasport
- Backdoor.Boda

File creation template

```
%TEMP%\uid.ax
%%TEMP%%\%s.ax
%%TEMP%%\%s _ p.ax
```

Command and control template

```
POST http://%ls:%d/%x HTTP/1.1
Content-Length: 2
CONNECT %ls:%d HTTP/1.1
Connection: keep-alive
lynx
```

There is also evidence that Backdoor.Vasport and Trojan. Naid have shared the same packer to obfuscate the payloads from AV detection. The obfuscation tool used is also Chinese in origin and has a simple user interface to help pack these Trojans.

Naid also has a history of using stolen digital certificates to overcome trust-based protection when attacking certain hardened targets. Some of the certificates identified are shown in Figure 22.

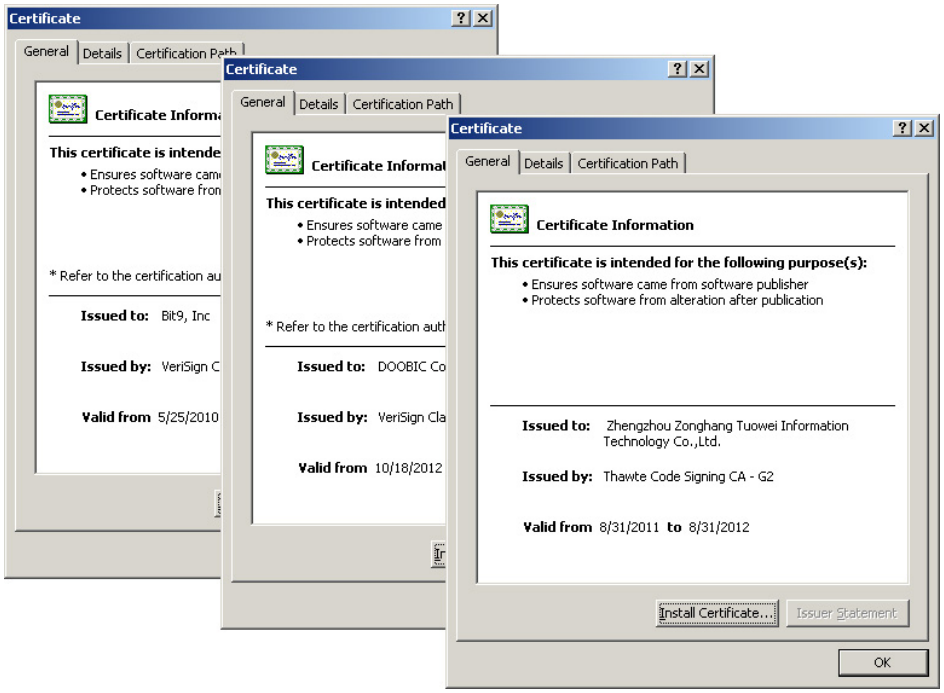


Figure 22. Stolen digital certificates used by Trojan.Naid

Backdoor.Vasport

Backdoor.Vasport was delivered by exploiting the Adobe Flash Player CVE-2012-0779 Object Type Confusion Remote Code Execution Vulnerability (CVE-2012-0779). This was delivered in malicious Word documents in targeted attack emails. The exploit component used in these attacks was also used in the Elderwood Platform.

Table 2 shows the payload from the malicious word documents.

Table 2. Backdoor.Vasport payload from malicious Word documents

PE Timestamp	MD5	C&C
27/04/2012 22:07	6fe1634dce1d095d6b8a06757b5b6041	svr01.passport.serveuser.com

Backdoor.Boda

In a more recent campaign called Ladyboyle, Backdoor.Boda was being distributed to take advantage of the Adobe

Flash Player CVE-2013-0634 Remote Memory Corruption Vulnerability (CVE-2013-0634). These files were signed with a digital signature from MGAME Corporation, a tactic used previously by the attackers. Interestingly, Backdoor.Boda and Backdoor.Vasport were both distributed using Flash zero-day exploits in embedded documents. It's plausible that the group has a team dedicated to distribution using Flash exploits that customizes Trojans from the same code base that the Naid uses.

Trojan.Hydraq (Operation Aurora)

The Hidden Lynx group has used cutting-edge attack techniques and a consistent methodology. Trojan.Naid has been in use since 2009 and Hidden Lynx attacks bear the hallmarks of a campaign that involved yet another Internet Explorer zero-day exploit in December 2009. Trojan.Naid was used in the infamous attacks on organizations in the financial, technology, Internet and media sectors called "Operation Aurora". These attacks are linked with another Trojan called Trojan.Hydraq, but Naid was downloaded in stage three of the operation.

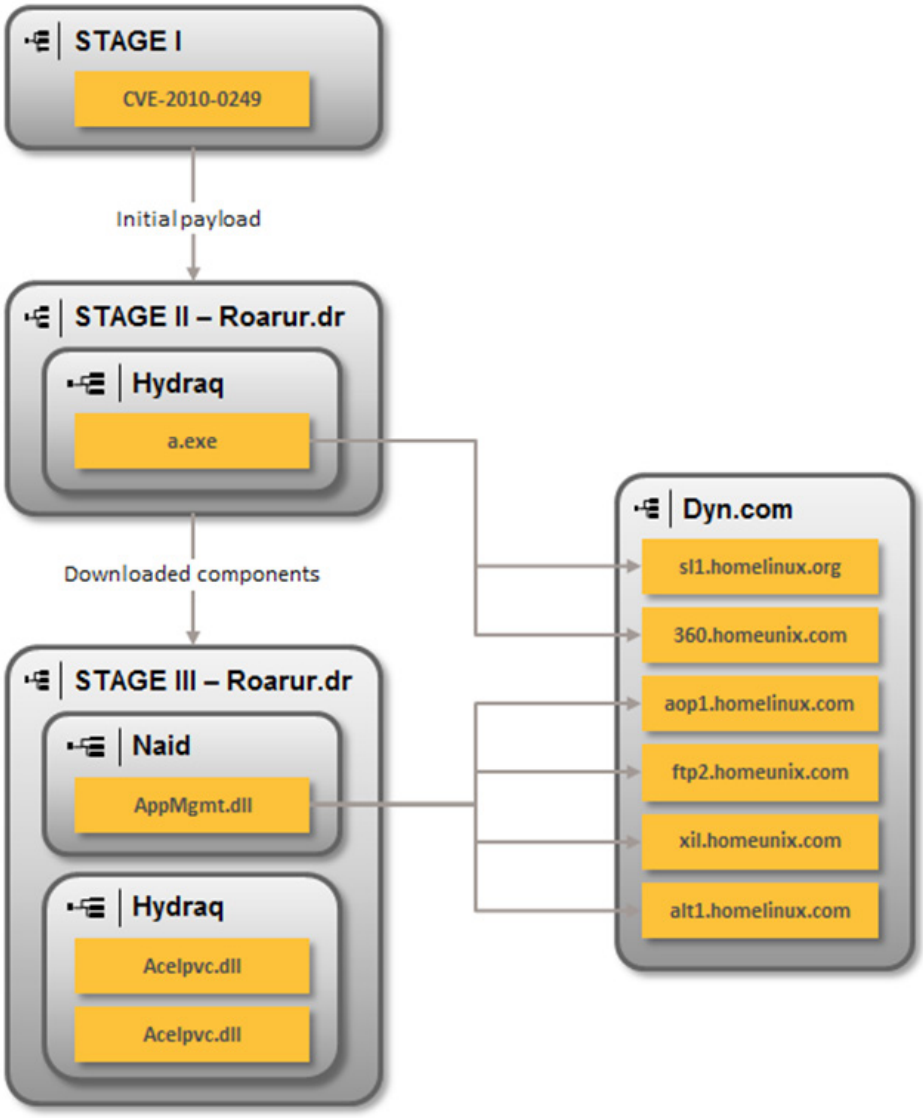


Figure 23. Trojan.Naid links to Hydraq and Operation Aurora

Trojan.Hydraq disappeared from the targeted attack landscape shortly after Operation Aurora, most likely due to the close attention that it was receiving from security researchers. Trojan.Naid did not meet the same fate, as it is still being used in sophisticated targeted attacks to this day.

Resources

- http://www.symantec.com/connect/blogs/hydraq-attack-mythical-proportions
- http://googleblog.blogspot.ie/2010/01/new-approach-to-china.html
- https://blog.bit9.com/2013/02/08/bit9-and-our-customers-security/
- https://blog.bit9.com/2013/02/25/bit9-security-incident-update/
- http://www.symantec.com/security_response/writeup.jsp?docid=2012-082113-5541-99
- http://www.symantec.com/security_response/writeup.jsp?docid=2012-061518-4639-99
- http://blogs.rsa.com/wp-content/uploads/VOHO_WP_FINAL_READY-FOR-Publication-09242012_AC.pdf
- http://threatpost.com/why-watering-hole-attacks-work-032013
- http://www.symantec.com/connect/blogs/latest-java-zero-day-shares-connections-bit9-security-incident
- http://www.cio.com/article/732122/_Aurora_Cyber_Attackers_Were_Really_Running_Counter_Intelligence
- http://www.infowar-monitor.net/2009/09/tracking-ghostnet-investigating-a-cyber-espionage-network/
- http://www.symantec.com/security_response/writeup.jsp?docid=2012-051606-5938-99
- http://www.symantec.com/connect/blogs/elderwood-project
- http://www.symantec.com/connect/blogs/adobe-zero-day-used-ladyboyle-attack

Symantec Protection

Many different Symantec protection technologies play a role in defending against this threat, including:


	Symantec Endpoint Protection	Norton 360	Norton Internet Security	Norton Antivirus
File-based protection	✓	✓	✓	✓
Network-based protection	✓	✓	✓	✓
Behavior-based protection	✓	✓	✓	✓
Reputation-based protection	✓	✓	✓	
Norton Safeweb		✓	✓	
Download Insight	✓	✓	✓	
Application & device control	✓			
Browser protection	✓	✓	✓	✓

File-based protection (Traditional antivirus)

Traditional antivirus protection is designed to detect and block malicious files and is effective against files associated with this attack.

- Trojan.Hydraq
- Backdoor.Moudoor
- Trojan.Naid
- Backdoor.Hikit
- Backdoor.Vasport
- Backdoor.Boda

Network-based protection (IPS)

Network-based protection in Symantec Endpoint Protection can help protect against unauthorized network activities conducted by malware threats or intrusion attempts.

- Web Attack: Oracle Java Rhino Script Engine CVE-2011-3544 (24700)
- Web Attack: Oracle Java Rhino Script Engine CVE-2011-3544 3 (24917)
- Web Attack: MSIE Same ID Property CVE-2012-1875 (25787)
- Web Attack: MSIE Same ID Property CVE-2012-1875 2 (26485)
- Web Attack: MSIE MSXML CVE-2012-1889 (25783)
- Web Attack: MSIE MSXML CVE-2012-1889 2 (50331)
- Web Attack: MSIE MSXML CVE-2012-1889 3 (25786)
- Web Attack: MSIE MSXML CVE-2012-1889 4 (25986)
- Web Attack: Java CVE-2012-1723 RCE (26051)
- Web Attack: Java CVE-2012-1723 RCE 2 (26080)
- Web Attack: Oracle Java Type Confusion Attack CVE-2012-1723 4 (25962)
- Web Attack: Oracle Java SE CVE-2012-1723 Remote Code Execution Vulnerability 3 (25934)
- Web Attack: Java CVE-2013-1493 RCE (26556)
- Web Attack: Java CVE-2013-1493 RCE 2 (26525)

Behavior-based protection

Behavior-based detection blocks suspicious processes using the Bloodhound.SONAR series of detections

Reputation-based protection (Insight)

- Norton Safeweb blocks users from visiting infected websites.
- Insight detects and warns against suspicious files as WS.Reputation.1

Authors

Stephen Doherty
Senior Threat Intelligence Analyst

Jozsef Gegeny
Software Engineer

Branko Spasojevic
Sr Software Engineer

Jonell Baltazar
Sr Software Engineer

About Symantec

Symantec protects the world's information and is the global leader in security, backup, and availability solutions. Our innovative products and services protect people and information in any environment—from the smallest mobile device to the enterprise data center to cloud-based systems.

Our industry-leading expertise in protecting data, identities, and interactions gives our customers confidence in a connected world. More information is available at www.symantec.com or by connecting with Symantec at go.symantec.com/socialmedia.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Follow us on Twitter
@threatintel

Visit our Blog
http://www.symantec.com/connect/symantec-blogs/sr

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527-8000
1 (800) 721-3934
www.symantec.com