White Paper

Threat Spotlight:
Angler Lurking in the Domain Shadows

Over the last several months Talos researchers have been monitoring a massive exploit kit campaign that is utilizing hijacked registrant accounts to create large amounts of subdomains for both initial redirection and exploitation. This campaign has been largely attributed to Angler Exploit Kit serving various malicious payloads.

The use of hijacked accounts lead to a larger research project into the use of hijacked registrant accounts. During this research the earliest examples were found from a 2011 campaign with sporadic usage until December 2014. Since December 2014 more than 75% of the subdomain activity has occurred indicating a major shift in approach.

Executive Summary

Angler is currently the best exploit kit on the market. The security industry has been waiting in anticipation to see which kit would replace “Blackhole”. While Angler may not have replaced Blackhole in terms of volume, the high level of sophistication and widespread usage leads us to declare Angler as the winner. It has shown the capability of integrating new exploits, including 0-days, quickly and effectively. With a new technique we’re calling **Domain Shadowing**, Angler has shown it is working hard to avoid standard detection.

Domain shadowing is the process of using users domain registration logins to create subdomains (i.e. says.imperialsocks.com). Angler Exploit Kit has begun utilizing these hijacked domain registrant accounts to serve malicious content. This is an increasingly effective attack vector since most individuals don’t monitor their domain registrant accounts regularly. These accounts are typically compromised through phishing. The threat actor then logs in with credentials and creates large amounts of subdomains. Since a lot of users have multiple domains this can provide a nearly endless supply of domains. Talos has found several hundred accounts that have been compromised that have control of thousands of unique domains. We have identified close to 10K unique subdomains being utilized. This behavior has shown to be an effective way to avoid typical detection techniques like blacklisting of sites or IP addresses. Since this campaign has done an exceptional job of rotation not only the subdomains, but also the IP addresses associated with the campaign. Additionally, these subdomains are being rotated quickly minimizing the time the exploits are active, further hindering both block list effectiveness and analysis. This is all done with the users already registered domains. No additional domain registration was found.

This recent campaign has been running since late December and coupled with the recent Flash 0-day has shown to be a new evolution in exploit kits. Utilizing 0-days and advanced evasion techniques were once reserved for targeted attacks and are now being packaged as the next evolution in the productized industrialization of hacking. This illustrates how products like Angler have raised the bar for the effectiveness of user driven exploit frameworks putting it in the same arena as the advanced threat market. Previously, the information security industry has been

trying to focus on detecting the threats like common, user targeted attacks while taking an “its not if, but when” approach to the advanced threats. Angler is now in the category of “not if, but when your organization will be impacted.”

Domain Shadowing

Attackers have been phishing for domain accounts to create large amounts of malicious subdomains for some time. This technique has not been covered in detail before so a new descriptive term needed to be created, **Domain Shadowing**. **Domain shadowing** is the process of gathering domain account credentials in order to silently create subdomains pointed at malicious servers without tipping off the actual owner. Talos has been able to identify hundreds of accounts that have been compromised, some for a year or more. Not surprisingly, the majority of the domains are held by GoDaddy which controls almost a third of the active domains.

The compromised accounts have several thousand domains assigned to them, however Talos has observed that only approximately a third of them have been utilized. This indicates that the actors still have a large reserve of domains and based on the data keep leveraging new accounts.

Fast Flux vs Domain Shadowing

Similar to Domain Shadowing, Fast Flux is a technique that rapidly changes the IP address associated with a domain to evade detection and blocking techniques. Fast Flux rotates a single domain or DNS entry to a large list of IP addresses rapidly. Domain Shadowing rotates subdomains associated with a single domain rapidly. These subdomains can point to a single IP or a small group of IP addresses depending on the circumstances. Below is a diagram illustrating both processes.

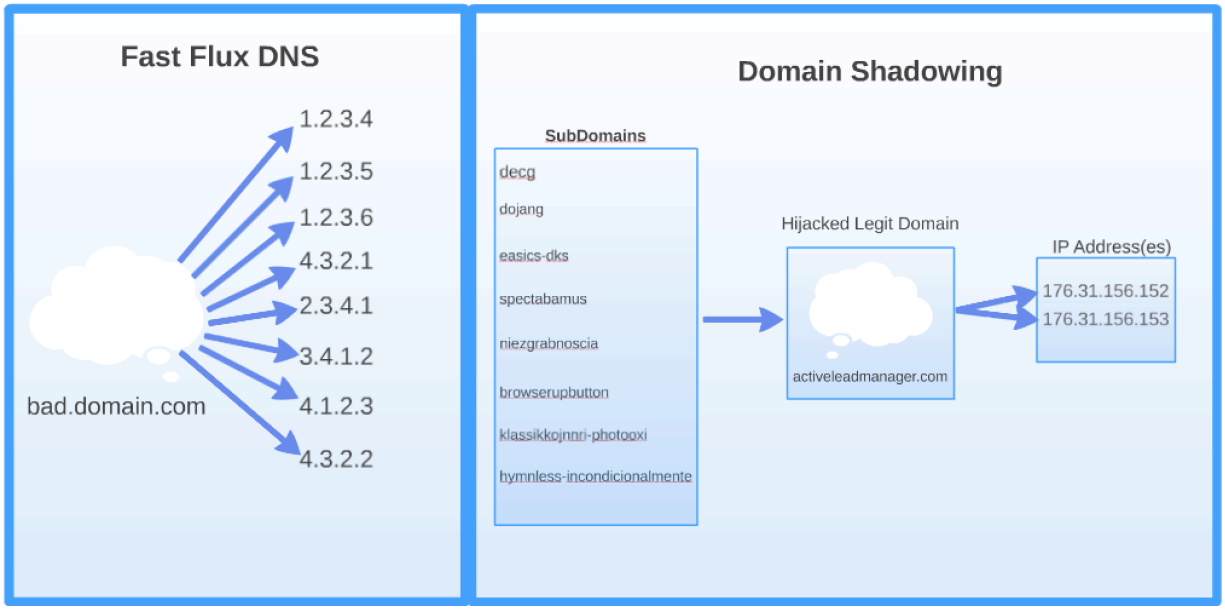

Figure 1. Illustrating Difference between Fast Flux DNS and Domain shadowing

History of Domain Shadowing

The first behavioral evidence that Talos found dates back to September 2011. At that time, a group of related domains were seen creating a large amount of subdomains. In the span of 45 days, approximately 15% of the total amount of identified subdomains were created. Most of the subdomains were active for less than a day and saw fewer than ten hits. The subdomains were constructed using randomly generated strings such as acajbehhcef.mysupercouponzz.info. These are characteristics that would resurface in later campaigns but with a much higher volume and quicker rotation. These particular domains were privacy protected so specific attribution was not available. They were, however, registered through GoDaddy something that would be a common theme throughout.

Until mid 2014, there was sporadic subdomain usage including a brief smaller campaign using the domains mentioned above. However, there weren't any significant campaigns that Talos found in its telemetry data. In May 2014, a new campaign started that was part of a browser lock campaign. The commonality of this campaign was the creation of *police* and *alertpolice* subdomains. These subdomains were created to serve the notification to compromised systems and provide payment details. Talos saw multiple domains associated with multiple different domain accounts being utilized during this period. This was also where some of the domain accounts that appeared in the recent campaign were first used for malicious purposes.

Fast forward to the campaign focused around the Angler Exploit Kit. The scope and amount of activity has continued to grow since the original post and was the starting point for this research. Including the most recent activity, more than 75% of the overall subdomains seen have occurred in this recent campaign. This campaign has been seen exploiting both Adobe Flash and Microsoft Silverlight vulnerabilities. The diagram below illustrates the growth of activity until mid-February. A larger bubble indicates more supportive events. December 2014 and on are the largest individual months in the last several years of activity.

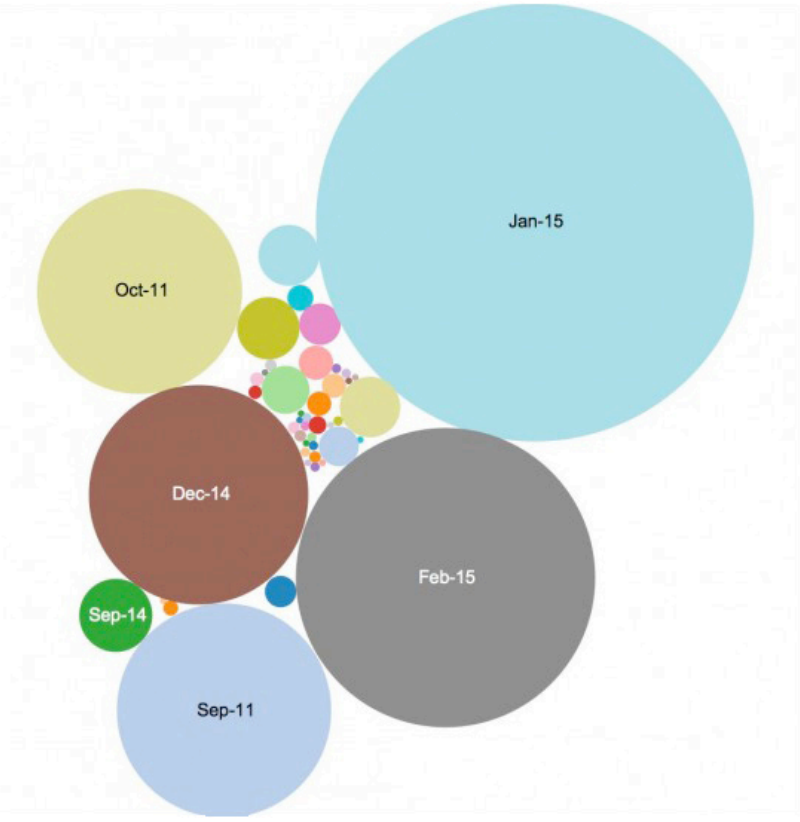

Figure 2. Illustrating explosion of usage since December-2014. Larger bubble indicates more events. (As of mid February)

Analysis of Subdomains

Talos identified a series of characteristics common to the recent subdomain creation, including multiple tiers of malicious subdomains. The first tier is responsible for the redirection to the actual exploit kit landing page. So far, there has not been any overlap between the domains utilized for the first tier and the exploit tier. There has also not been any overlap in the domain accounts that are utilized.

The amount of subdomains being utilized for landing pages and exploits are greater than those used for redirection, by a factor of five. This could be related to the chain of events leading to compromise. The user browses to a web page that is hosting a malicious ad. The malicious ad redirects the user to the first tier of subdomains (commonly referred to as a "gate"). This page then redirects to the actual landing page serving exploits. This final page is being rotated at a rapid pace. Some of the subdomains are only active for a matter of minutes and only are reached a couple of times.

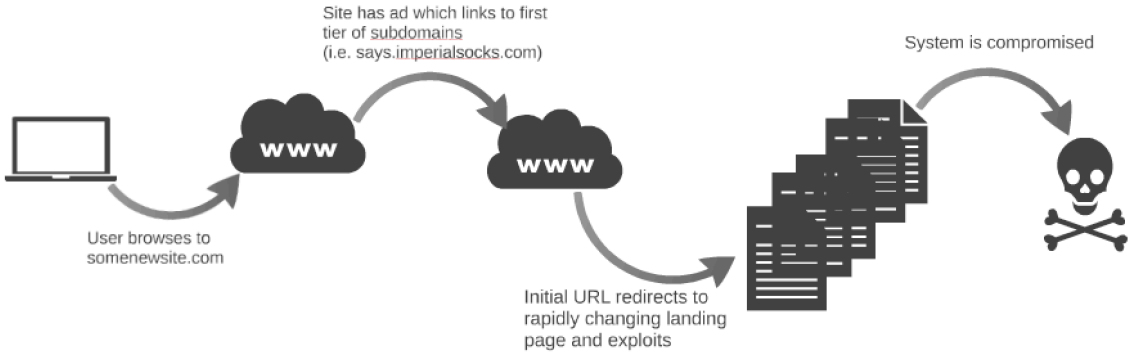

Figure 3. Attack Chain for Exploit Kit Campaign

There are some other differentiators between the redirecting domains and the exploit domains. The redirecting domains only made use of third level domains that were english word based (i.e. says.imperialsocks.com). The landing page / exploit kit subdomains are random string based and recently have branched into using both third level and fourth level domains (i.e. brandmuellergekwantifiseer.astarentals.co.uk & 3e3qcq.plante.bplawfirm.net)

From an IP address perspective the same IP is utilized across multiple subdomains for a single domain and multiple domains from a single domain account. There are also multiple accounts with subdomains pointed to the same IP. The addresses are being rotated periodically with new addresses being used regularly. Currently more than 75 unique IP's have been seen utilizing malicious subdomains.

Patterns have also emerged with the domain accounts that are being leveraged. Accounts with multiple domains usually have more than one domain being actively leveraged. However, none of the accounts have reached 100% saturation so among the accounts with multiple domains there are still unused domains reserved, potentially, for later use. The amount of accounts has continued to grow. New accounts were seen as recently as mid February and based on the growth there could be a substantial amount of accounts still to be seen.

The one thing all these accounts have in common is the registrar: GoDaddy. Based on recent data, GoDaddy is the registrar for almost a third of the domains on the Internet and is nearly four times the size of the number two registrar. If a group is going to take the time to create a phishing campaign this would be the registrar to target, and the data Talos has found indicates that is the case.

Exploit Kit URL History

This use of Domain Shadowing is the most recent evolution that exploit kits have gone through to evade detection and remain active and effective for as long as possible. In their infancy, exploit kits and other malicious threats made use of hard coded IP addresses for the malicious content. This is obviously a flawed methodology since a simple blocklist add would eliminate it from being effective.

The next iteration was to start registering domains to be used for the exploit. This allowed for the server to be changed easily to try and avoid detection a little longer. The downside was that the actors needed to register the domains which allowed researchers to investigate and potentially find new domains that had not yet been used. Next up was the use of dynamic DNS (DDNS), which Talos has covered previously. This allowed actors to stand up new domains anonymously and quickly. This is quite effective and is currently in use with some exploit kit activity.

Domain shadowing using compromised registrant credentials is the most effective, difficult to stop, technique that threat actors have used to date. The accounts are largely random so there is no way to track which domains will be used next. Additionally, the subdomains are very high volume, short lived, and random, with no discernible patterns. This makes blocking increasingly difficult. Finally, it has also hindered research. It has become progressively more difficult to get active samples from an exploit kit landing page that is active for less than an hour. This helps increase the attack window for threat actors since researchers have to increase the level of effort to gather and analyze the samples.

Detection

Detection of exploit kit campaigns using this technique is difficult due to the steps taken to avoid the more common detection methods. This again emphasizes the importance of a true defense in depth approach to security as some of the typical detection techniques will not succeed with this attack. The subdomains and IP's being used are changing regularly so typical blacklisting isn't nearly as effective as it would be normally. The actual samples being served are being morphed frequently which has hindered AV detection significantly (many samples with low detection). The keys to detection rely largely on NGIPS and advanced heuristic based malware detection. Most of these exploit attempts will trigger multiple NGIPS rules for generic Adobe Flash exploits, generic Silverlight exploits, and landing page detection. Additionally heuristic based malware detection software will detect the exploitation attempts as well as the post exploitation behavior.

There are a couple of other types of detection that may be effective against this threat. Looking for multiple subdomains resolving for a single second level domain. Additionally looking for multiple subdomains resolving to a single IP address. Finally looking for random string subdomains could be effective as well. However, this does present some challenges as there are lots of legitimate services especially cloud based hosting that make use of quasi-random subdomains causing high FP rates.

IOC

For IOC's please visit http://cs.co/9004NcGg.

Conclusion

User's are at risk for these types of attacks because they are designed to evade detection and prevention. A malicious ad can be hosted on virtually any website causing compromise. These random domains that are hosting the exploits are difficult to identify and anticipate. This coupled with 0-day attacks has shown to be an extremely successful methodology with compromise. This particular campaign is unique in its large scale use of Domain Shadowing.

The process of Domain Shadowing is effective not only because it makes blacklisting difficult but also leverages that most users only login to their domain registrar to renew the registration. This threat example clearly demonstrates the ongoing evolution of threat actors. Actors are always going to try and stay ahead of detection technologies, and increasingly the researchers.

This latest campaign has successfully elevated Angler to an advanced exploit kit. One that utilizes 0-day's and evasion techniques that were previously associated with advanced threats alone. At this point its more a question of "when" Angler will affect you instead of "if". If you are relying exclusively on blacklisting technologies, this threat is designed to beat it. Utilizing multiple products with different inspection engines can help ensure the most comprehensive coverage before, during, and after the attack.

Angler related Snort Rules: 28613-28616,29066,29411-29414,30852,31046,31129-31330,31331-31332, 31370-31372,31694,31695,31898-31901,32390,32399,33182-33187,33271-33274,33286,33292

For the most up to date list, please refer to Defense Center or FireSIGHT Management Center.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA CXX-XXXXXX-XX 10/11