Exploit Evolution and Advanced Threats

Over the last year exploit kits have begun evolving and earning a reclassification as advanced threats. A true shift from basic to advanced threats is underway, everything from adware to exploit kits are adding techniques and methods commonly found in those threats previously labeled as APT. These methods include support for 0-days, advanced evasion techniques such as domain shadowing, and anti-reversing technologies such as VM-aware malware and increasingly short attack windows, moving and changing quickly. The fact that these capabilities, once reserved for an elite few, are now available effectively to the public has taken the exploit kit arms race to the next level.

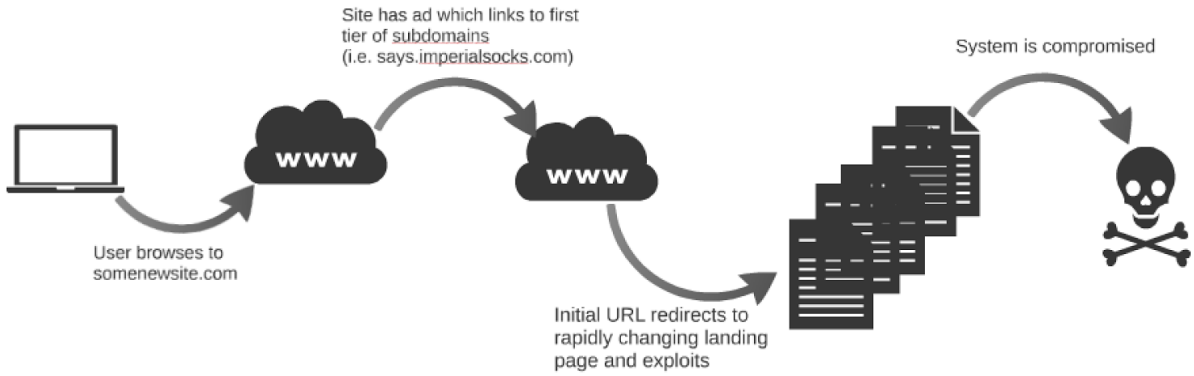
Exploit Kits have been a common part of the threat landscape for the better part of a decade. Initially the kits were largely driven by common exploits being served to unsuspecting users via compromised web sites. Recently we have started to see a major shift in sophistication, which is part of the larger monetization of hacking, that occurred over the last year. This started with exploit kits adding support for lesser-known vulnerabilities as evidenced by Angler Exploit Kit being the first to serve Silverlight based exploits. At the time Silverlight was not being widely exploited and was the first of several changes that were led by Angler. Shortly after Angler added Silverlight all other exploit kits, that hoped to stay relevant, had included support.

Then in late 2014 Angler lead the way again this time integrating an Adobe Flash 0-day into its framework. Again it was the first and all other exploit kits followed shortly. Another change that occurred during this time was the advent of domain shadowing. Domain Shadowing is the process of leveraging compromised registrant accounts, specifically from godaddy, to create malicious sub domains. There are several advantages to this tactic, first is that you are not required to confirm an email address, which is now an ICANN requirement. It makes it much more difficult to shut down since the domains are chosen at random and are much more difficult to identify in advance. The attackers are taking advantage of the fact that users do not regularly check their registrant accounts and therefore wouldn't notice the accounts being created. This campaign lasted for several months, covered thousands of domains tied to hundreds of unique godaddy accounts. Toward the tail end of the campaign Talos observed RIG exploit kit starting to leverage this same technique. The final and most effective aspect of Domain Shadowing is its effect on blacklisting technologies.

Talos has observed more than twenty-five thousand subdomains being utilized. If the primary detection technology being used involves blacklisting this attack will not be stopped by it, its too high of a volume moving at light speed. This is part of a larger trend Talos has been observing across multiple different attack vectors, evasion. Talos has seen threats designed to defeat a single type of detection technology, whether it be blacklisting as in this example, or Anti-Virus or NIDS/NIPS, threat actors are actively working to defeat a single technology increasing the importance of layering protections.

One final change has been the attack window and distribution method. Talos has observed the amount of time a single site is active and hosting the landing page of

exploit kit has gone from days down to minutes. The sites are being rotated on an almost constant basis, with the IP addresses also being rotated at a slower pace. The reason this type of behavior is available is because of a shift in distribution method. Previously, exploit kits were largely delivered via compromised sites, like wordpress sites. Now with the explosive growth of malvertising these exploit kits can be delivered to users leveraging banner ads, which can be changed and rotated rapidly. This not only allows attackers to shorten the attack window for a single URL, but also reach a much wider audience with a built in distribution methodology. At a high level malvertising is just making use of an existing infrastructure, but instead of serving a normal legitimate ad the malicious actors will serve either an exploit directly in the banner ad or redirect the user to a redirection tier, known as a gate, and then redirect the user to actual landing page to be compromised. Below is an image, which shows the attack chain at a high level, specifically involving domain shadowing:



This evolution of exploit kits in conjunction with the trend in adware to include VM aware functions and the explosion of ransomware shows how attackers are changing. Previously these characteristics were reserved for attacks that were labeled as advanced persistent threats or APTs. Now Talos has seen these sophisticated elements start to make there way into the lower tier of threats. This can partially be attributed to the explosion in the money available via hacking enterprises. This has led to fully functional organizations with development groups and budgets to make their products stand out from the competitors. Its this fundamental change has led to the gap narrowing between these previously isolated classes of malicious activity.