Targeted Network Attacks

June 2011
Michael Cotton, CISSP
Chief Network Security Architect
Vulnerability Research, Digital Defense, Inc.

Digital Defense Whitepaper
9000 Tesoro Drive, Suite 100 | San Antonio, Texas 78217 | www.ddifrontline.com

Introduction

In recent years, companies have made substantial investments into their information security infrastructure. IT auditing, widespread anti-virus deployments, and other network-based defense mechanisms have had a major impact on the detection and eradication of typical Internet-based malware threats.

These investments notwithstanding, companies are still often not aware of a more significant threat to their network: network attacks that are targeted specifically for their organization.

This whitepaper attempts to give a broad overview of some common methods used by hackers during targeted network attacks and some steps an organization should take to combat them.

Background

Targeted network attacks are attacks created and customized to penetrate a specific target or organization. They share a number of characteristics that make them unique from typical Internet based malware. These attacks:

- Focus exclusively on a single organization
- Are typically preceded by heavy reconnaissance of the target network
- Often use payloads specifically tailored for the target network
- Leverage published trust relationships and social engineering that exist within the organization
- Are not typically geared towards traditional monetization schemes

The problem most organizations have with preparing for these types of threats is that they often assume that the random Internet-wide malware they frequently encounter represents the extent of all threats that exist.

What companies fail to realize is that not only are they not being specifically targeted by most Internet-based malware operations, but given the choice, the authors of most modern malware schemes would prefer to avoid large enterprises, and their associated security teams, altogether.

Consider the following recent news story about a fake antivirus scheme:

"Three men have been charged over a 100 million dollar scam involving fake-antivirus software… if guilty they could face up to 20 years in prison for each charge, along with a $250,000 dollar fine - and prosecutors are calling for a $100 million deposits in European banks to be handed over as well" [1]

When malware authors can leverage these types of scams to make large amounts of money by extracting small incremental amounts across millions of home users in an automated fashion, the hassle and risk of attempting focused corporate network penetrations for direct monetary gain, is not worth their effort or the risk of exposure. Simply put, there are easier ways to make money from malicious and illegal activity on the Internet.

That said high-profile targeted network attacks have clearly exploded in recent years with high-profile network breaches occurring almost weekly. Consider the following recent examples:

1) Sony PSN Hack Exposes 77 million subscribers data [1]
2) RSA Security SecureID breach [2]
3) Theft of Comodo SSL certificate root signing key [3]
4) Stuxnet attacks against Bushehr nuclear reactor in Iran [4]
5) Morgan Stanley Aurora network breach [5]
6) HBGary network breach by 'Anonymous' [6]
7) Canadian government breach of state secrets from attacks originating in China [7]

The attackers involved in the above incidents had a wide variety of motives; some political, some strategic, some military, but in all cases, money was not the primary motivator for these high profile incidents.

Examining the HBGary network breach in particular is illuminating as this is a rare case where the attackers gave interviews about how and why they performed this targeted attack. An overview of the incident is as follows:

1) HBGary Federal CEO Aaron Barr announces he intends to 'unmask' members of the hacktivist group 'Anonymous' at a security conference in San Francisco.
2) 'Anonymous' responds by launching an operation with the ultimate goal of destroying HBGary Federal via cyber attacks.
3) Reconnaissance is performed against HBGary's Internet-facing systems.
4) It is determined that one of the systems is vulnerable to an SQL-Injection attack; this is leveraged to download a set of password hashes from the web application.
5) Password hashes are cracked, and then these credentials are leveraged against other services running on Internet-facing systems.
6) Other systems fall to a combination of password re-use and local privilege escalation, credentials on these systems are then cracked as well.
7) All acquired credentials are then used against HBGary's main corporate email account (hosted on Google apps) and one account yields Administrator access.

8) Attackers download HBGary's entire corporate email archive.

9) Attackers use social engineering attacks while representing themselves as HBGary employees to gain access to other websites that cannot be penetrated with pure network attacks.

10) Attackers publish HBGary's entire email archive online, deface and then shut down HBGary's Internet-facing systems, and disclose details of the attack to the media.

It is important to note that this attack could have been carried out at any time in the past with a similar degree of success. However, until Aaron Barr challenged the group 'Anonymous', the company maintained a low threat profile and thus their apparently inadequate security controls were 'good enough'.

Most companies will look at an example such as the HBGary incident and assume that the way to avoid a devastating breach is simply to 'not pick fights' with groups such as 'Anonymous', or consistently maintain a low threat profile. This is easier said than done.

At a large organization with thousands of employees and a national or multinational presence, it is very difficult to ensure no actions are taken that might cause the companies threat profile to rise. Among the myriad of actions known to precipitate attacks, here are a few examples:

1) Political contributions to specific groups or causes.

2) Cease and desist letters sent to websites.

3) Refusing to do business with specific organizations (i.e. Wikileaks).

4) Positions on Internet-centric issues such as net neutrality.

5) Bold claims about the unbreakable security posture of a company or its products.

6) Website 'takedown' notices or legal threats sent to end users.

7) Negative national media attention from some action taken by company.

While most organizations realize the impact of these events on public relations, these same organizations do not recognize the increased threat to their organization's web sites and networks. An assumption exists that because malware and random attacks have been stopped before, any new attention generated by the event will simply result in increased, but still failed attempts at infiltration. This is the equivalent of assuming that because a soldier on the battlefield has not been hit by a stray bullet, a sniper now taking aim at him presents no greater threat.

Targeted Attack Methods

Targeted attacks are by their very nature, unique to the organization at which they are directed. While it isn't possible to ascertain ahead of time the manner in which an organization might be breached, there are a common set of vectors and goals that often show up. These goals can be broadly defined as follows:

1) Attempt to establish a foothold on either an Internet-facing system or client machine on the internal network.
2) Pivot further attacks through this system to take advantage of internal network access and/or trust relationships.
3) Install a Trojan program or advanced persistent threat mechanism to ensure continuous access to the targeted network.

The first goal focuses on gaining some basic level of access to a device, which can then be leveraged to breach other devices. This initial level of access is often the greatest obstacle to overcome for an attacker, as future attacks can leverage both trust relationships that go along with email accounts and the greater level of network access granted to a company's equipment.

Common methods of achieving this access often focus on client applications, which interact with data as it comes through the firewall. While some methods of remote server exploitation are still effective, they are not so common that an attacker can expect to consistently find these on an organization's external network.

Email messages with Trojan attachments continue to represent the most common and effective exploitation vector for an attacker to gain an initial foothold inside the network. Adobe PDF attachments, Microsoft Office Files, and hyperlinks within email messages are things that clients are accustomed to receiving and opening from external sources. As such, they require a very low 'trust' threshold to facilitate their opening.

While Microsoft and Adobe have introduced a number of security mechanisms to attempt to mitigate this classic attack, recent security research proves that these mechanisms can be reliably defeated. [1]

From a social engineering perspective an attacker will often try to craft a payload in such a way that people are immediately enticed to open the associated attachment, but quickly lose interest without becoming suspicious of the contents that it contains. Any further communication on the contents of the attachment to other employees within the organization can often result in alarm bells being raised, making further network penetration substantially harder as employees are warned about the nature of the threat.

The fundamental goal the attacker has at this initial step is to both entice people into opening their payload and to ensure the communication does not result in any additional communication within the organization. Messages which are too enticing will often result in additional internal communication, raising concern within the organization. On the flipside, messages which attempt to appear so bland that nobody is interested in talking about them run the risk of not being opened at all.

Examples on both extremes that penetration test teams have been known to use:

1) Organization Announcement - Layoff Notice: 100% click through rate, 0% chance of evading detection.
2) Summary of proposed changes to comply with upcoming Sarbanes Oxley Regulations: 0% click through rate, 100% chance of evading detection.

Ideally, an attacker is attempting to find some message which a user feels immediately compelled to open but quickly dismisses as unimportant and closes. Messages portraying themselves from ISPs or accounting firms are ideal candidates for this type of spoofing as organizations have 'loose' established trust relationships with these entities. These relationships are frequently a matter of public record, and employees feel obligated to read the communications from these entities even though they often turn out to contain mundane details which require no further action.

While crafting payloads to use against a specific organization, malware authors often will tailor their payloads to bypass defense mechanisms that organization is known to have in place. Often times, details on the defense mechanisms used by a particular organization are easy to come by. Job posting by employers for IT personnel, or resumes posted by current employees often enumerate the various security technologies at play within a specific organization. Security logos placed on vendor or partner websites are often an unintentional disclosure of the particular defense mechanisms a targeted attacker might wish to evade.

What many people don't realize is just as anti-virus systems sell their ability to detect malware; Trojans and other malware threats often similarly advertise their ability to evade antivirus systems. The reason for this misconception is easy to see; IT personnel are constantly inundated by advertisements for defensive security technologies but rarely are in the market for a rootkit, so they only hear one side of the argument. Unfortunately, evasion for a sophisticated attacker is both common and often part of their standard tool set.

Consider the following screenshot advertising rootkit evasion:

[1] Rootkit Detection Testing

The following detection tools were tested in April 2007. A subset were retested in August 2008. The rootkit was installed prior to the detection tool.

AVG AntiRootkit 1.0.0.13	RAIDE Beta 1.0
Bit Defender v8	Red Pill
BlackLight 2.2.1055	RootKit Unhooker 3.01
DarkSpy 1.05	RootkitBuster 1.6-1049
GMER 1.0.12.12011	RootKitDetector 0.62
Helios 1.1a	RootkitRevealer 1.71
Hook Annalyzer 2.00	Sana Security SafeConnect 2.1.0
IceSword 1.20	Sophos Anti-Rootkit 1.2.2
Kproc Check .2beta2	Spybot S&D 1.4
McAfee Virus Scanner 2007	SunBelt CounterSpy 1.5.82
McAfee Stinger 2.60	System Virginity Verifier 2.3
Norton AntiVirus 2007	Trend Micro 2007 15s1329
Norton Internet Security 2007	VICE 2.0
Process Hunter 1.0	Zone Alarm Pro
Process Walker 1.04	Kaspersky Internet Security

[source: arstechnica [8]]

In this case the rootkit in question was not advertising its ability to evade any single security technology so much as its ability to simultaneously evade nearly every security technology it was likely to encounter.

Consumer Reports has garnered a large amount of controversy in the past for testing anti-virus systems by using standard obfuscation techniques on existing malware variants to see how systems fared when confronted with malware they had not seen before. However, the fundamental objection many in the security industry seemed to hold was that the behavior of obfuscating existing virus samples was 'irresponsible', not that the testing method was invalid. [9]

Unfortunately, security is maybe the one industry where you cannot say "but that's unethical, illegal, or irresponsible" in objecting to an opponent's tactics. This is not a courtroom; there are no rules for criminal behavior. There are a variety of valid responses to concerns raised about the efficacy of a security product when confronting a particular problem but "that's not fair" should never one of them.

Companies also commonly deploy in-band network monitoring tools as secondary breach detection mechanisms. Intelligent firewalls, Intrusion Detection and Intrusion Prevention Systems are often technologies that organizations invest in. While these systems do have their place, the same payload obfuscation mechanisms that fool anti-virus systems present a challenge for these systems as well.

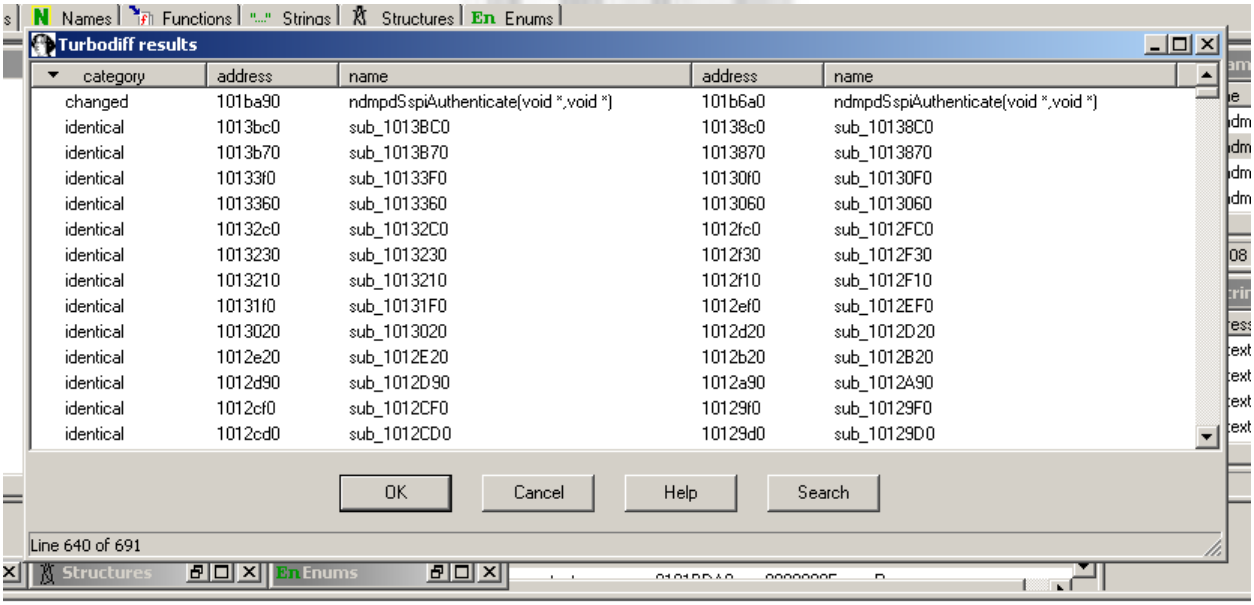
Once a system has been compromised by a Trojan, the ability of these technologies to detect stealthy outbound command and control communications can be severely limited. Just a few additional packets representing themselves as HTTPS traffic or DNS requests (as in the case of the Conficker and Stuxnet Worms) during normal web browsing usage present a very difficult problem for in-band detection mechanisms to flag. The days where Trojans would only attempt to establish outbound connections to port 31337 over unencrypted channels are long gone.

Even for companies that practice due diligence through routine vulnerability assessment and patch management, the current pace at which exploits now deploy proves to be an ever-increasing challenge.

The modern reverse engineering tool-chain frameworks have gotten so advanced that the process of extracting an exploit vector from a vendor patch has been reduced from days to hours, and in some instances, minutes.

For example, the following screenshots were taken during reversing a patch last year to examine the nature of a particular flaw. For the purposes of demonstration, I used only free tool-chains; in this case IDA Pro 4.9, and TurboDiff.

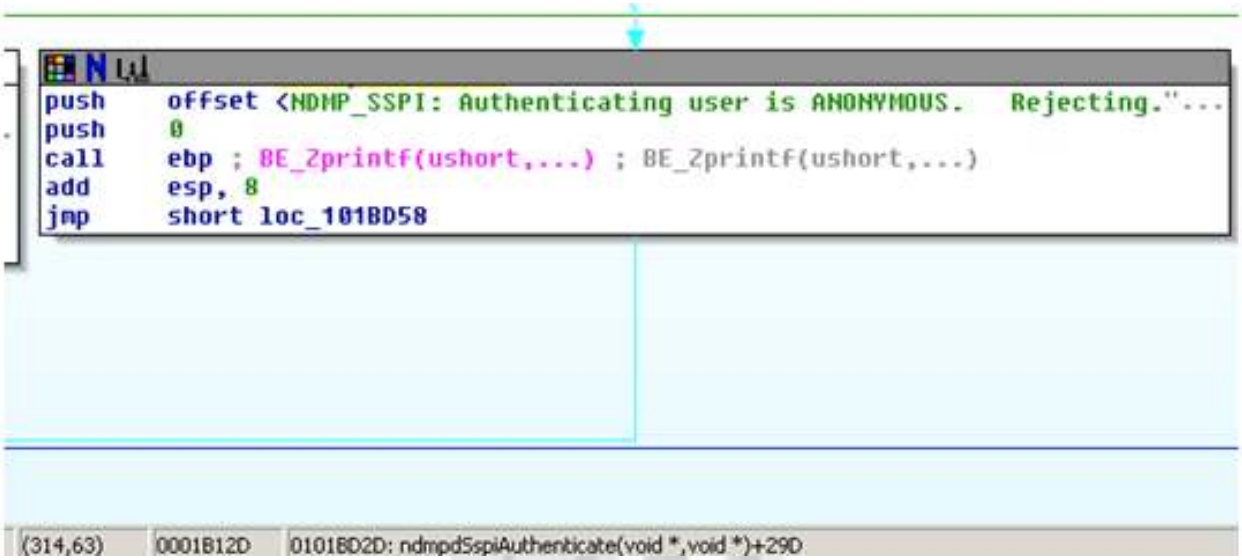
The process starts by doing a binary diff of the un-patched and patched binaries in order to see what functions have changed:



Once this has been accomplished. you can drill into the function to get an overview of the extent of the changes. From the above table we can see a single function has

changed and it's a good bet our authentication bypass resides here as the name of the function is "ndmpSspiAuthenticate".

Drilling into this code, the nature of the authentication bypass flaw becomes quickly clear. The patched binary has inserted a new block of code which specifically rejects Anonymous SSPI tokens during authentication.



Therefore an attacker can quickly conclude that unpatched versions of this software will accept Anonymous SSPI tokens during the authentication sequence; granting unprivileged users privileged access. More about SSPI interfaces can be viewed here:

http://en.wikipedia.org/wiki/Security_Support_Provider_Interface

Through techniques like these, advanced attackers can often utilize attacks based on newly released patches before a target organization is even aware of the need to update.

Solutions

The most important thing to realize when attempting to secure a network against targeted attacks is that there is no magic bullet. Security vendors will often position their products as such but any honest security vendor will portray their product as something that mitigates security risk but will never reduce it entirely. As the sophistication of the attacks targeting your network increases, the extent to which standard defensive tool-chains can help mitigate the threat drops off dramatically.

One of the most important things you can do is to understand that because targeted attacks so often leverage sophisticated social engineering, employee training is a critical aspect of any security program. Organizations often make the mistake of simply

reading off a laundry list of things not to do; e.g. "Don't give out your password" rather than presenting more realistic scenarios. A better tactic is to train employees by presenting real-world examples of successful social engineering attacks against the behavior the company is trying to prevent.

Another common gap in security controls is that companies often leave security training as an annual exercise for the sake of efficiency. This tends to have the effect of putting new hires on the network without any security training whatsoever. Because these employees tend to be younger and more junior in position, they represent ideal targets for attacks such as these as they are less likely to push back against someone representing themselves as an authority figure in a social engineering attack. By building security training into the new employee orientation process, organizations can often eliminate these types of mistakes.

Probably the single, simplest thing an organization can to improve its security posture is to reduce the attack surface of its standard client configurations by ensuring that software with a poor security record and no real business application is simply uninstalled. For example, how many people really need Shockwave Flash installed in their browser at work? Is it something that employees 'need' to have or just something that they find nice to have for casual web surfing?

An active vulnerability management program can assist in not only identifying vulnerabilities in various pieces of software but in identifying various services running on each machine. IT departments can leverage these results to not only ask "why is this service not patched" but also "does this service need to be running at all"? One of the most frequent observations made by clients when looking at the results of a vulnerability assessment showing weaknesses in their network is "that's funny we don't even use that (service/application/device)".

A vulnerability management program that incorporates both regular scans and semi-annual penetration tests is also critical to locating any other areas where security controls might be lacking. By effectively implementing a strong security program with the sorts of techniques presented above, an organization can gain a much greater understanding of which security controls are not working and ways to best correct any deficiencies in order to efficiently minimize overall risk.

References

1. http://www.pcworld.com/article/227297/sony_faces_weekend_hack_attack_report_claims.html
2. http://www.tgdaily.com/business-and-law-features/49985-three-charged-over-massive-fake-anti-virus-scam
3. http://www.thetechherald.com/article.php/201111/6941/RSA-s-SecurID-targeted-in-data-breach

4. http://www.wired.com/threatlevel/2011/03/comodo_hack/
5. http://www.schneier.com/blog/archives/2010/10/stuxnet.html
6. http://news.softpedia.com/news/Morgan-Stanley-Targeted-in-Operation-Aurora-187037.shtml
7. http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars
8. http://news.techworld.com/security/3261707/china-denies-role-in-canada-government-hack/
9. http://arstechnica.com/tech-policy/news/2011/02/black-ops-how-hbgary-wrote-backdoors-and-rootkits-for-the-government.ars
10. http://redtape.msnbc.com/2006/08/consumer_report.html