The Getaway:

Methods and Defenses for Data Exfiltration

Sean V Coyne

Sean (dot) Coyne (at) MANDIANT.com

January 2011

Abstract

This white paper discusses the methods and advanced tactics attackers use to steal data, and the countermeasures victims can take to defend against these activities. Since the turn of the century cyber crime has become less about destruction and reputation, and more about taking what is of value and maintaining secrecy. There are several stages to a successful cyber attack. The most crucial, yet least discussed is data theft. Every class of attacker has a way to compromise your network and find what they want. While there are several tools, methods, and strategies to combat intruders, the reality is that once they have made off with your data there is no getting it back. The game is over.

MANDIANT's consultants regularly respond to incidents where data, intellectual property, and even money are being stolen from victim organizations. During this presentation we will take a look at some of the advanced data theft techniques we have seen attackers use. We will review how they prepare staging areas, avoid DLP/traffic scanning products, and how the attackers use the victim's own infrastructure and architecture against them. Finally, we will discuss why these tricks work and what, if anything, can be done to stop them.

The Getaway: Methods and Defenses for Data Exfiltration

Introduction

MANDIANT is an information security company providing incident response, computer forensics, penetration tests, education and software to Fortune 500 companies, financial institutions, government agencies, domestic and foreign police departments and several of the U.S.'s leading law firms. MANDIANT consultants are experts at Incident Response who have responded to over one hundred incidents and performed reviews on hundreds of thousands of potentially compromised machines.

Because of the skills and experience of MANDIANT's investigative teams we are often called on to perform complex computer forensic in support of intellectual property cases, data leakage, inappropriate use, computer intrusions and merger & acquisition matters. It is in drawing from this vast experience that we put together this briefing on the most cunning data theft techniques we have seen.

The methods discussed in this paper often involve custom malware created by talented developers. The attackers who use this type of malware are well organized, well prepared teams who know what they are after. An examination of both the simple and sophisticated methods used here and the possible countermeasures organizations can take to defend against them should be valuable to anyone charged with protecting data.

That Word Doesn't Mean What You Think it Means.

In military jargon exfiltration is the removal of personnel or units from areas under enemy control by stealth, deception, surprise, or clandestine means. In computing terminology, exfiltration refers to the unauthorized release of data from within a computer system. This includes copying the data out through covert network channels or the copying of data to unauthorized media [3]. Data exfiltration is one of the last stages of a successful cyber attack along with removing evidence and maintaining access to the systems; however, it is the most crucial.

Is it clandestine or covert, let's differentiate between those terms. 'Covert' means "to conceal the source of". So when a 'covert action' takes place, generally its results will be readily known but the identities of the actors are obscured. 'Clandestine' means that the action itself will remain a secret and its having been carried out should remain unnoticed.

In regard to data exfiltration, security professionals use the terms interchangeably and neither is wrong. Attackers work to keep their breach of victim systems undiscovered. They do what they can to confound investigators by removing logs and files once they've been exported. They also frustrate attribution efforts by using various techniques and servers in multiple countries. For our purposes we will use the term 'covert'.

Why Do We Care?

The one and only thing of value that resides on a network is the data. Whether it is personally identifiable information (PII), financial details, credit card numbers, trade secrets, source code, or some form of intellectual property; it is what an attacker has expended effort to obtain and it is what the organization likely has a significant financial interest in keeping secured.

At the point an attacker gains access to the network it is still anybody's game. Until the attacker locates what is of value on your network and packages and removes it, there is still the opportunity to stop the attack and seal the breach before anything is lost. Organizations' networks may be probed or attacked regularly but, depending on local laws, they are not required to notify anyone until data has been taken. Even if the attack is only discovered once the data exfiltration is already in progress the opportunity remains to cut off access and limit the exposure.

Many organizations overly stress the importance of network perimeter security: firewalls, intrusion prevention systems, strong authentication, and patch management. Despite this, more organizations are compromised each year then can even be reported, many companies suffer breaches and don't know until the data has left the target environment and shows up out in the world. The methods attackers use are not typically the latest slick 0-day or some advanced hack; typically organizations are breached by phishing emails, client-side exploits or just poor configuration. Attackers will also craft their movements to appear benign in logs. This is done by choosing ways to connect to the target network that are the same ones used by regular employees such as through legitimate remote access applications that exist for user convenience. So the attacks will look no different to the IT staff than legitimate employees connecting remotely for business.

Not nearly enough emphasis is placed on internal network traffic monitoring – especially lateral movement from workstations to workstations, and workstations to servers. Similarly, although many organizations use web proxies and firewall rules to control internet egress traffic, it is far too easy for modern backdoor communications to blend in with normal user activity. Paying close attention to the behaviors of "normal" activity against "standard" systems by establishing network traffic baselines is the key to identifying a problem before it is too late. Every anomaly should be viewed with a degree of suspicion and addressed through internal investigation or, if necessary, reviewed by an outside expert. Otherwise, once the network is breached the attackers will have their run of the system. The people responsible for network security should assume attackers will find a way in.

How to Get it Moving!

Covertness is a characteristic of a data exfiltration operation which can be measured by the rate of usage of the medium. And so the measure of covertness is a function of utilization of the capacity for a given medium. If the medium of exfiltration is utilized at its maximum capacity,

the operation is easily visible with a covertness of zero. If instead the medium is exploited at a lesser rate, the operation will be increasingly covert. Therefore, to keep an activity as covert as possible, the rate of usage relative to the capacity of the equipment should be kept as low as possible. The greater the consumption of bandwidth, CPU cycles, or storage space for staging files, the less likely the data exfiltration will remain unnoticed.

Once the internal network has been mapped and the pertinent files located, the attacker will begin packaging the data into a less cumbersome format. This is typically done with standard password protected archive file types: RAR, ZIP and CAB files. These file types are not uncommon on most computers so they are one less thing that can stand out and attract attention. One thing IT security personnel can do to overcome this is to be on the lookout for such archiving tools placed in unusual directories. For example a search of the network for 'rar.exe' would return many false positives, but searching for 'rar.exe' outside of its standard installation directory may yield interesting results. Also, since attackers are likely to remove their tools once they are done, investigators could also search for references to 'rar.exe' in system restore point change logs or check Windows prefetch for indications that 'rar.exe' was frequently run.

The next step is collecting the data in one or a very few staging areas to await transport. The fewer outbound connections making file transfers the less noticeable the exfiltration will be. Connection from within the network to the system being used as a staging area will likely go unnoticed without internal traffic monitoring. Loading all of the packaged data into an obscure folder on a little used system with plenty of extra storage allows the attacker plenty of freedom and room to work with. Attackers can survey the network at their discretion, move the files to one collection point and wait for the right time to remove the data. Once it comes time for the attackers to remove the data from the network it will be far easier and faster to manage the exfiltration.

Finally, it's time to move the data out. The ports and protocols used may vary but there is always one objective: to go unnoticed. This can be achieved in one of two ways. The first is to protect or obscure the data transfer with some type of tunneling protocol or encryption. The second is to make the traffic blend in with the normal everyday flow of data from the network. This is done by taking advantage of what is already in place in the infrastructure: open ports on firewalls, web servers, RDP, FTP servers, etc. As stated earlier, the advantage here is that it becomes very difficult to separate the attacker's traffic from employee traffic and customer's legitimate business.

Just How Bad Can it Be?

Cyber crime is certainly on the rise – reports increased by 22% in 2009 to 336,655. Out of this number only 146,663 were forwarded to authorities [2]. It is virtually impossible to attach a dollar amount to the loss due to data exfiltration. This is because the value of what was taken has not even been realized in the marketplace yet. It is also impossible to estimate a loss of market share due to competitors obtaining trade secret and loss of stock value if a victim is required to disclose there has been a breach. A precise figure for amount of data lost cannot be

determined because many organizations never report the crime, cannot determine how much data was taken, and may not even know they have suffered a data loss.

One of the most significant cases seen by MANDIANT involved a client that suffered a multi-phase attack over the course of several months. Once an attack was detected and the client tried to remediate, the attackers would activate previously unused accounts/backdoors, re-infect and continue their data exfiltration with modified methods. In the last investigation, our forensic analysis identified 105 compressed multi-part RAR archives totaling over 120 gigabytes of data created by the attacker, all spread across six compromised systems used as staging areas.

Case #1: Naked file transfer through RDP

In our first case, MANDIANT identified tunneled remote desktop traffic entering into the client environment. From there, drives were received for forensics; analysis of network logs indicated that the compromised server was not communicating to other IP addresses at the time.

Upon review of the drives. MANDIANT identified the attacker logged into the network server using Microsoft Remote Desktop (RDP) and created multiple files on the system called '.eml' files – the default extension for Microsoft Outlook Express mail files. The prefetch entries indicated that the first use of Microsoft Outlook Express had been while the attacker was logged on to the system. Basically, the attacker opened the mail file which contained no headers but contained the mime-encoded attachment. When viewed within Outlook Express the attacker could save the attachment which could contain whatever tool he may be uploading or data being exfiltrated.

Review of log files indicated that there were no other connections to the server at the time and no e-mails had been sent, thus investigators concluded that the '.eml' files were created and moved by the attacker through the copy-paste functionality embedded within RDP Terminal Services. Once the e-mail file had been created with its attachment the attacker could open the '.eml' file in a hex editor, copy-paste the raw data to his local machine and recompose the '.eml' file. While this can be turned off on RDP "web" clients, this cannot be turned off through Microsoft Remote Desktop Client application.

Case #2: Malware checks its Webmail

In our second case, the attackers were able to gain access to the compromised system. Attackers then transferred a program called 'webmail.exe' to the system and attempted to run the executable file. This command-line based tool used a hard-coded username and password to connect to a public webmail account via https. It used the webmail account to post and retrieve information, providing the attackers with the capability to upload stolen files as attachments. In short, the attackers were e-mailing themselves the data upon logging into the account. To keep from drawing attention to itself the malware had a fixed wait time of nearly eight hours between connection attempts. The network traffic generated by this compromised host would be

indistinguishable from a user's normal webmail session. MANDIANT investigators have seen this done using Yahoo, Hotmail, and Gmail accounts.

The question here is why not simply run e-mail programs like Eudora or ThunderBird? Webmail services are built to be able to interface with these programs over Pop3 or IMAP. The answer is simply that the attackers strove to be as minimally invasive as possible. Installing new programs and creating new connections that used protocols, even common ones, which might be filtered or noticed would not be acceptable. Webmail, like all http/s traffic, flows over port 80 and 443 allowing the attackers' data exfiltration traffic to blend in with all the rest.

MANDIANT investigators were able to find this malware through monitoring the system, which their investigation had led them to identify as infected. In this case, host-based analysis to find both the backdoor malware as well as the webmail utility was a critical first step. Once the network traffic of the infected system was being closely monitored it was easy to recognize the pattern as being highly suspicious. The pattern followed as: contact to identified Malicious IP – Webmail – Malicious IP – Webmail – etc. Once again the attempt here was to blend in with normal user traffic and go unnoticed.

Case #3: Down the Tunnel, through the Loop

In our third case we take a look at an organization that has suffered persistent pressure and reoccurring compromises by attackers. This example of advanced data exfiltration occurred in the second round of compromises. In this round the attacker compromised several servers with a variant of the well known 'Poison Ivy' malware. Once they had access back into the network, the attackers found and compromised two servers running unused instances of Microsoft Internet Information Services (IIS). Once these two servers with IIS running were taken control of they were loaded with a custom protocol tunneling malware. Once this malware was in place the attackers created a tunnel from their machines to the IIS servers. It was at this point that the .rar files that had been staged on another server were moved to the web root of the compromised IIS servers. Once the files were in place the attackers could retrieve the data via http download. Attackers activated their protocol tunnel to the IIS servers, then from there browsed to port 80 on the same server they were tunneled to and retrieved the files.

The effect of this was to create in the logs the appearance that the IIS servers were sending GET requests to their own localhost port 80. To further conceal the movement of the data, the attackers had a third tool in place to scrub the IIS logs of any entries with references to .rar files in them. Thus, the logs were scrubbed of the evidence but not fully deleted. Missing logs would have been too much of a tip off. These logs were found by a MANDIANT analyst who managed to catch the attackers in the middle of the act, retrieve the unedited logs and discover the malware. The obvious lessons here are that unnecessary or unused services should not be running on servers, egress points should be monitored for any suspicious traffic, and log data should be streamed, stored and reviewed regularly. Of course administrators must know what is normal before they can notice what is abnormal or suspicious, so once again network traffic baselines become critical.

References

1. Giani, A. Berk, V. Cybenko, G.(2007). *Data Exfiltration and Covert Channels*. Thayer School of Engineering, Dartmouth College, Hanover, NH 03755 USA

2. Percoco, N. (2010). *Data Exfiltration: How Data Gets Out.* SpiderLabs

3. "Exfiltration - Wikipedia, the free encyclopedia." *Wikipedia, the free encyclopedia*. 2011. <http://en.wikipedia.org/wiki/Exfiltration>.

4. Mirko Zorz -, and 27 October 2009.. " Q&A: Malware threats, Windows 7 and cyber crime." *Help Net Security*. N.p., n.d. Web. 11 Jan. 2011. <http://www.net-security.org/article.php?id=1336&p=2>