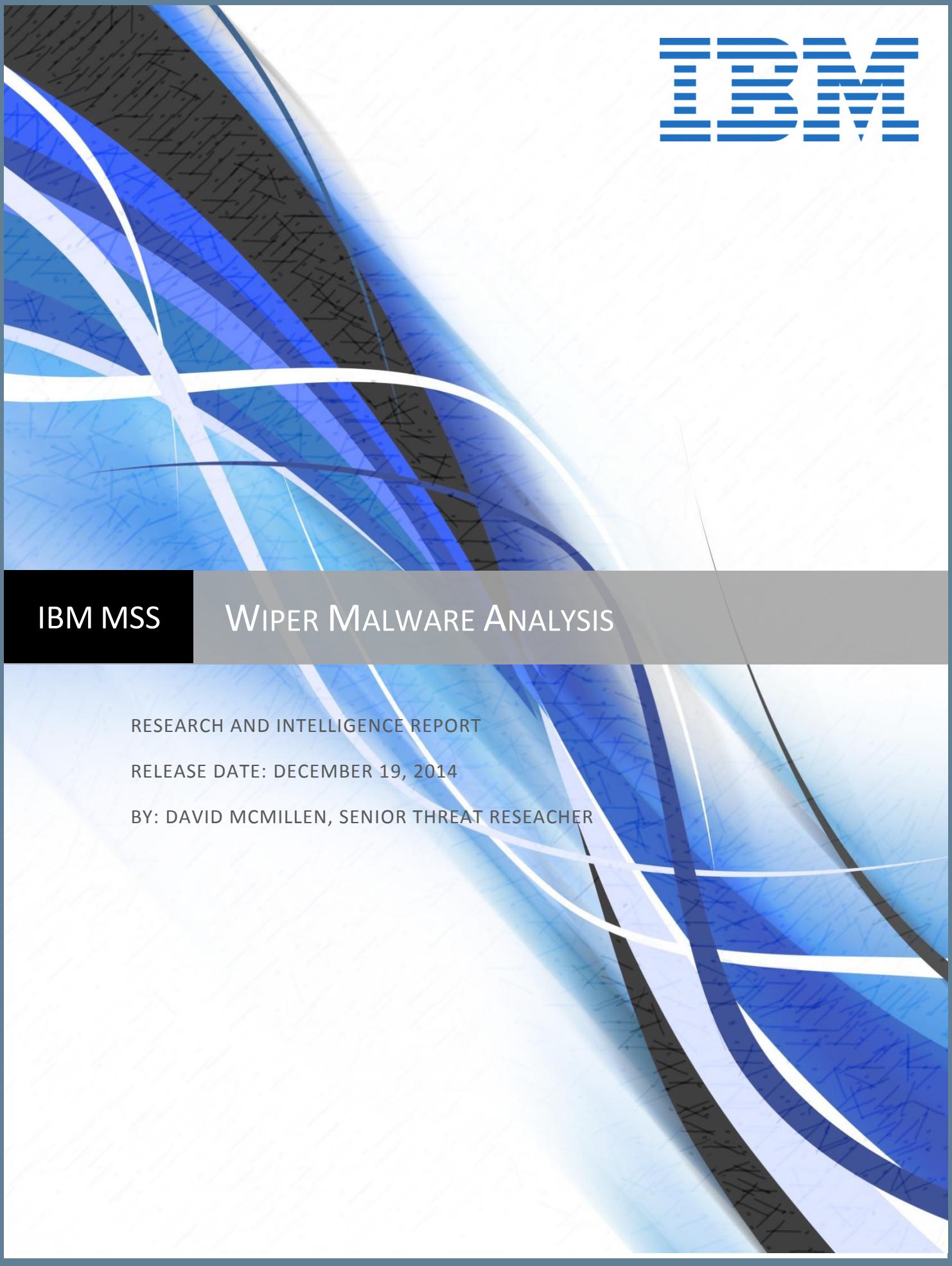


IBM MSS

WIPER MALWARE ANALYSIS

RESEARCH AND INTELLIGENCE REPORT

RELEASE DATE: DECEMBER 19, 2014

BY: DAVID MCMILLEN, SENIOR THREAT RESEACHER

TABLE OF CONTENTS

EXECUTIVE OVERVIEW/KEY FINDINGS

This past November, news wires were full of stories concerning a data breach at Sony Pictures Entertainment (SPE). What became clear in the days after was that a powerful piece of malware named Wiper was to blame. The post analysis of Wiper showed that, not only was it dropped into Sony's network without detection, it also communicated with a command and control network which it utilized to send the contents of the victim's hard drive. Once that task was accomplished, the malware then destroyed the drive contents using a "bootkit" designed to erase the content and delete the master boot record. This prevents the machine from booting back into the operating system.

Interesting connections exist with the wiper malware we examined. Three of the seven wiper type malware objects have a tie directly to South Korea (Koredos, Dozer, and Jokra) and three more have ties directly to Iran (Narilam, Maya, and Shamoon). The seventh has been potentially tied to North Korea (Destover).

This type of attack is not new. In the past few years there have been numerous attacks using that same objective. This paper takes a look at those past incidents, dives into the details of similar "Wiper" type malware as well as looks into who is responsible for these types of attacks.

WHO IS USING THIS ATTACK?

Security experts are indicating that for the most part, the "Wiper" attacks are largely being executed by insiders, hacktivist groups, and nation states. In the case of Sony, it was first thought that North Korea was to blame because the malware samples retrieved from the Sony network contained code that had ties to that country. As the investigation progressed, it became clear that Sony's situation may have been primarily caused by an insider.

Some of the hacktivist groups known to perpetrate these types of attacks are the #GOP (Guardians of Peace) which took primary responsibility for the Sony breach, the Cutting Sword of Justice who breached the oil company Aramco using a wiper type of malware called Shamoon in August 2012, and a group called Dark Seoul who used a coordinated attack to "wipe" data from several banks and media companies in Seoul, South Korea back in May 2013.

Can these attacks be considered cyberwar? If a nation state is not behind these attacks then cyber-terrorism should be the primary consideration. Targeting critical infrastructure almost always points to

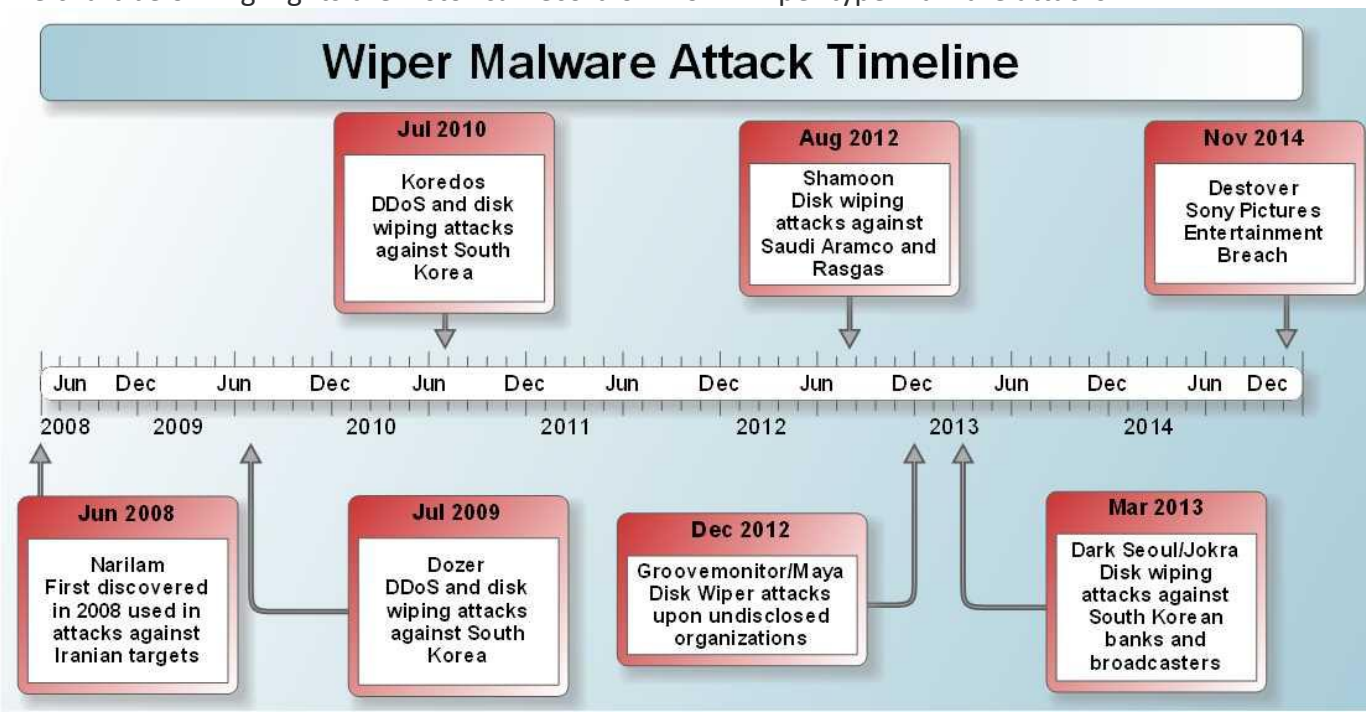
cyber-terrorism. Stuxnet was a cyberwar campaign that went on for years and was perpetrated in a very stealthy method. The Wiper attacks are very loud and are focused on a couple distinct industries pointing to a less determined adversary, more than likely, hacktivist groups.

What is clear is that these large scale attacks focusing on cyber-destruction have some very strong similarities regardless of who is perpetrating them, indicating some groups may be working together with a common interest. The insiders who have helped to pull off these successful attacks may also have ties back to the same groups.

HISTORY OF WIPER MALWARE

Although the Sony breach this past November continues to make headlines, due in large part to the data loss that has also occurred, it is important to note that destructive malware has had quite a sordid history over the past few years. With the advent of this latest news, this type of attack will more than likely become extremely popular over the next few months. While some wiper type attacks have taken place solely with the intention of destroying a target's digital assets (more than likely due to political reasons), we can expect a fair amount of electronic extortion to pick up in intensity as we have seen with Sony breach. This incident definitely fits the bill as a mega breach and just may be the largest of its kind in history. That kind of evil success story will almost surely encourage other hactivist groups to engage other targets across multiple industries utilizing this attack vector.

The chart below highlights the historical record of known wiper type malware attacks.



POPULAR TYPES OF WIPER MALWARE

The wiper malware highlighted in the timeline above is discussed in detail below.

NARILAM

This malware affects databases for some very specific software packages which are mostly used in Iran. The disk corruptions Narilam promotes are extremely subtle and are very difficult to notice. If allowed to run for months or years, the effects can be quite destructive as the modifications are extremely hard to detect. Narilam was specifically designed to be slow acting in order to perpetrate long term sabotage. There are several versions of Narilam which date back to 2008. The Iranian Maher Cert Team published an alert about Narilam back in 2010 stating that the targets could not be disclosed but, in November 2012, the Iranian company TarrahSystem indicated they were experiencing Narilam attacks. Reports from Kapersky indicate that the malware was mostly found in Iran (60%) and Afghanistan (40%).

Narilam focuses on these specific applications:

Maliran Integrated Financial and Industrial Applications
Shahd (Nectar) Integrated Financial / Commercial Software
Amin Banking and Loans Software

DOZER

Dozer is a wiper type malware that is spread primarily through email. It was first seen being utilized in an attack against the United States and consisted of DDoS and wiper type attacks against South Korea and U.S based government and financial web sites on July 4, 2009. Dozer was unique because it implemented a time bomb mechanism. The time bomb was to execute on July 10, 2009. The bomb was designed to overwrite specific file types and then finally overwrite the first one megabyte of the victim's drive, destroying the master boot record and partition table. The hard drive was overwritten with the string "Memory of the Independence Day".

KOREDOS

In July of 2010, a major wiper type malware attack took place focused on business web sites in South Korea. Not much is known about the victims as details were never disclosed. Koredos contains a mechanism to destroy the master boot record of the host drive it infects. It was also found to contain a Trojan dubbed Backdoor.Prioxer which was very sophisticated and infected files in a discreet manner. The backdoor contains a dynamic link library file that acts as a botnet component utilizing IRC as its main communication method. The bot acts to exchange commands and data with a command-and-control server (C&C).

GROOVEMONITOR/MAYA

A very crude wiper type malware. First reported in 2012 by the Iranian Maher Cert, this malware triggers on specific dates that are hardcoded which range from December 10, 2012 to February 4, 2015. When a specific date is reached, the malware simply deletes all the files on drives “d:” through “i:”.

SHAMOON

In August 2012, approximately 30,000 computers at Saudi Aramco were wiped and rendered unbootable by a hactivist group named “Cutting Sword of Justice”. The malware that was recovered was dubbed Shamoon. Similar to Groovemonitor/Maya, this malware used a crude method to wipe and destroy the hard drives. Shortly after Saudi Aramco was hit, the same type of attack was focused on the Rasgas company in Qatar. It was first thought that Iranian hackers were behind these attacks because an artifact found in the malware contained a string that mentioned “Shamoon for Arabian Gulf”. Some security researchers disagree due primarily to the fact that Iranian programmers would have dubbed this “Persian Gulf”.

DARK SEOUL/JOKRA

In March of 2013, a group known as Dark Seoul began attacking several banks and broadcasting companies in South Korea with DDoS attacks. Simultaneously, the group was also successful in dropping a Trojan called Jokra into their networks. Jokra first disables antivirus and security processes before it begins to inventory all the network drives beginning with the primary drive. It also searches for network drives that are not mapped with a drive letter. Once it has a list of targets, it begins to overwrite the master boot records of all the drives. The malware then executes a command line shutdown command. When the machine reboots, the drives are rendered useless without a full format and restore. The Dark

Seoul group is also responsible for a four year campaign of cyber terror beginning in 2009 that included the use of both the Dozer and Koredos Trojans which rewrite the MBR of the victim's drive.

DESTOVER

In November of 2014, news of a data breach of major proportions was announced affecting Sony Pictures Entertainment. As details became available, it became clear that terabytes of data were stolen and the native drives destroyed. Subsequently, the data was held hostage by the Guardians Of Peace (#GOP) for ransom and, at the time of this publication, that situation continues. Destover has some major similarities to Shamoon. Interestingly, a backdoor named Trojan.Volgmer contained within Destover, contains a mechanism to communicate with a command and control server (C&C) which allows command execution, system information retrieval and file upload and download capability. The variants of Volgmer are configured to end execution if the compromised host is not located in Korea.

RECOMMENDATIONS/MITIGATION TECHNIQUES

Since wiper attacks are extremely destructive, simply deploying defensive tactics will never provide full peace of mind. Intrusion Prevention signatures and Antivirus solutions are simply not effective enough on their own to mitigate this type of attack. The following tactics should be utilized and stringently enforced.

- Isolate important intellectual property to hardened networks. Access only over privileged connections.
- Utilize off site data backups for critical information.
- Implement an emergency business continuity/disaster recovery plan and test at regularly scheduled intervals.

IDPS SIGNATURES AND/OR SIEM RULES

CISCO

Wiper Malware Activity
Shamoon Malware Activity

NETSCREEN

HTTP:WIPER-SHAMOON-FILE-DWNLD

PALO ALTO

Shamoon.Gen Command And Control Traffic
Shamoon.Gen Command And Control Traffic

SNORT

MALWARE-BACKDOOR Jokra dropper download
MALWARE-OTHER Win.Trojan.Narilam variant inbound attachment
MALWARE-OTHER Win.Trojan.Narilam variant outbound connection

SOURCEFIRE

MALWARE-BACKDOOR Jokra dropper download
MALWARE-BACKDOOR DarkSeoul related wiper

DESTOVER YARA RULE

```
rule unknown_wiper_error_strings{
meta: unique custom error debug strings discovered in the wiper malware
strings:
$IP1 = "203.131.222.102" fullword nocase
$IP2 = "217.96.33.164" fullword nocase
$IP3 = "88.53.215.64" fullword nocase
$MZ = "MZ"
condition:
$MZ at 0 and all of them
}
```

REFERENCES

Sony/Destover: Mystery North Korean Actor's Destructive and Past Network Activity
http://securelist.com/blog/research/67985/destover

Trojan.Koredos
http://www.symantec.com/security_response/writeup.jsp?docid=2011-030417-4602-99

Shamoon The Wiper: Further Details (Part II)
http://securelist.com/blog/incidents/57784/shamoon-the-wiper-further-details-part-ii

Narilam: A 'New' Destructive Malware Used In the Middle East
http://securelist.com/blog/incidents/34692/narilam-a-new-destructive-malware-used-in-the-middle-east-34

GrooveMonitor: Another Wiper Copycat?
http://securelist.com/blog/virus-watch/34811/groovemonitor-another-wiper-copycat

Trojan.Jokra
http://ae.norton.com/security_response/print_writeup.jsp?docid=2013-032014-2531-99

Destructive Malware – Five Wipers in the Spotlight
http://securelist.com/blog/incidents/58194/destructive-malware-five-wipers-in-the-spotlight/

DISCLAIMER

This document is intended to inform clients of IBM Security Services of a threat or discovery by IBM Managed Security Services and measures undertaken or suggested by IBM Security Service Teams to remediate the threat. The data contained herein describing tactics, techniques and procedures is classified Confidential for the consumption of IBM MSS clients only.