Anomaly Detection Challenges - Challenge V

Hamza Tahir (03670002) and Muhammad Hamza Usmani (03669506)

Technical University of Munich

1 Malware Report

This brief report serves as a purpose to present and explain the methodologies behind three particular malware strains, normally found to attack vulnerable systems.

2 Zeus-Citadel

2.1 What is the purpose of the malware?

It is a Trojan horse malware package. It has widespread usage but the primary usage is to steal banking information. It also facilitates the installation of ransomware.

2.2 Who is the actor?

It has widespread usage but in 2010, a lot of the activity was traced back to Eastern European hacker groups, who were subsequently arrested.

2.3 What are some interesting techniques used?

Mostly utilizes ”Man-in-the-browser (MITB)” or ”form grabbing” techniques. MITB refers to infection of a web browser with a program that modifies the data that passes through it. Form Grabbing is similar to this, where a browser is infected by retrieving authorization and log-in credentials from a web data form before it is passed over the Internet to a secure server

2.4 Was the malware tool successful?

Zeus, or its recent variant Citadel, has become the largest botnet on the Internet. From 2007, has been known to affect high profile targets such as the United States Department of Transportation and compromised over 74,000 FTP accounts on websites of such companies as the Bank of America, NASA, Monster.com, ABC, Oracle, Play.com, Cisco, Amazon, and BusinessWeek. So I would say it was pretty successful.

2.5 What did the defenders do wrong, right, or how did they respond?

Companies such as MalwareBytes and Damballa are well aware of the dangers Zeus-Citadel poses, and are consistently trying to educate people on getting their anti-virus software up-to-date. Even though the creator allegedly retired a few years ago, the FBI has said that it may be a ruse and he may come back. The source code of the original malware is now available. However, new variants pop up every now and then and no system is safe, even now.

3 Crypto-Locker

3.1 What is the purpose of the malware?

It is a form of Ransomware, wherein the malware encrypts the victims data using RSA public-key cryptography. The victim is then locked out and the only way to get access to his own data is via a ransom payment to the attacker.

3.2 Who is the actor?

Random attackers on the internet who want to extort people for money.

3.3 What are some interesting techniques used?

Mostly utilize social engineering techniques, such as emails that trick the victim into opening a zip file that installs the Trojan.

3.4 Was the malware tool successful?

Yes, the attackers successfully extracted $3 million from the victims, with 40% of the people affected eventually paying the ransom.

3.5 What did the defenders do wrong, right, or how did they respond?

What they got right was that they took payments via anonymous pre-paid cash vouchers (i.e. MoneyPak or Ukash), or an equivalent amount in bitcoin (BTC). That made them hard to trace.

4 Conficker

4.1 What is the purpose of the malware?

Conficker is a worm targeting the targets Windows. It uses flaws in Windows OS software and dictionary attacks on administrator passwords to propagate, and has been unusually difficult to counter because of its combined use of many advanced malware techniques, which include forming botnets.

4.2 Who is the actor?

Unknown.

4.3 What are some interesting techniques used?

The attackers seem to be combining a variety of very advanced malware techniques which, while individually well known to researchers, combined make the malware quite difficult to stop.

4.4 Was the malware tool successful?

The Conficker worm infected millions of computers including government, business and home computers in over 190 countries, making it the largest known computer worm infection since 2003. Yeah, pretty successful.

4.5 What did the defenders do wrong, right, or how did they respond?

The virus' authors are believed to be tracking anti-malware efforts from network operators and law enforcement and have regularly released new variants to close the virus' own vulnerabilities. This makes them an ever-changing opponent, thus hard to defeat.