The Battle Against Breaches

Going Beyond Signature Based Malware Detection

November 2013

www.csid.com

TABLE OF CONTENTS

THE BATTLE AGAINST BREACHES

GOING BEYOND SIGNATURE BASED MALWARE DETECTION

When it comes to protecting the personal information of employees and customers, and the company's intellectual property, businesses are losing. 2012 saw more than 47,000[1] reported security incidents, costing businesses $5.4 million per breach[2] in monetary damages - not including brand damages. With 2012 numbers coming in high and 2013 on track to be equally as disastrous, the question that becomes increasingly urgent is how do we fix this? What can businesses do to protect against the malware that is inflicting the bulk of these damages?

One in every three machines worldwide carries some variant of malware. A 2012 survey conducted by security firm Panda Labs, found that 32 percent of users had malware-infected devices. In China, more than half (54 percent) of devices were carrying a form of malware.

The process of malware fraud is simple. A fraudster sets up a malicious webpage with a domain name that is similar to a well-known site or injects malicious content into a legitimate site. Someone within a business then infects his or her computer with this malicious content. This can be done by clicking on a link in an email, on a website or even just visiting a legitimate website that is infected with drive-by malware. This malware then finds sensitive information – like employee login credentials or customer email addresses – and sends it to a central command and control server, where the stolen information is stored until the fraudster makes use of it.

The criminal can do a number of things with this newly stolen information. A common next step is selling it in a hacker chat room or on the Internet black market. Bundles of 100 emails and passwords can be sold for as much as $5. A Social Security Number and date of birth can go for as much as $20. A bank account with a balance of $10,000 can go for an average cost of $625. A credit card with full identifying information such as name, security code, expiration date and address can be sold for as much as $30.[3]

> *2012 saw more than 47,000 reported security incidents, costing businesses $5.4M per breach in monetary damages*

In a more alarming scenario, a criminal can take the employee information, which often includes a login and password, and use it to delve deeper into a company's system often accessing sensitive and valuable data, resulting in a data breach.

Signature based detection is one of the most common methods used to identify instances of malware on a device. The process works by scanning the contents of a device's files and then cross-referencing the content with known signatures belonging to variants of malware. If a signature match is found, then the file contains a virus. The software can then quarantine, delete or repair the file so it no longer poses harm to the system or the user.

Signature based detection has long been the core of many IT departments' cyber security efforts. In 2011, consumers and businesses spent a combined $7.4 billion on antivirus software. This is almost half of the $17.7 billion

[1] 2013 Data Breach Investigations Report, Verizon Enterprise
[2] 2013 Cost of Data Breach Study: Global Analysis

[3] CSID CyberAgent

spent on security software in 2011.[4] Yet numerous studies have shown that signature based detection methods are becoming increasingly ineffective. An analysis done by security reporter Brian Krebs found the detection rate of anti-virus software to be around 25 percent.[5] What this means to businesses – when an employee clicks on a malicious link or visits a website with malicious code, there is a one in four chance that the code will be detected – a three in four chance that it will slip by, unnoticed.

The reason for this is simple – signature-based detection is a reactive process and it is near impossible for anti-virus software companies to keep up. The rate at which malware evolves can be staggering. CSID alone detects more than 76,000 variants of malware, daily. Other security companies have seen between 200,000 and 300,000 new viruses daily.[6] These malware variants circulate in the wild for a very short time. For most malware, by the time it is detected, it is often out of circulation. Similarly, it is easy for hackers to hide the malicious code in packages that are then sealed like envelopes, making it near impossible for anti-virus software to detect.

ENTERPRISE THREAT INTELLIGENCE

Malware protection is a fundamental need for any business. Gartner anticipates that worldwide spending on security infrastructure will reach $86 billion in 2016, up from $60 billion in 2012. The growth of the industry illustrates and mirrors the rise and severity of attacks and how seriously businesses are taking the threat of breach.

To address this need and provide businesses with an effective supplement to signature based monitoring, CSID has developed a new system called Enterprise Threat Intelligence.

Enterprise Threat Intelligence does two things: monitors for and harvests compromised information that is being sold on the identity black market, and monitors for compromised IP addresses.

In 2012, **CSID's CyberAgent®** found:

- **19M+** Total Records
- **17M+** Emails
- **16M+** Emails with passwords

Monitoring for compromised information is done in real-time through CSID's proprietary CyberAgent® technology, which means a business can learn that an employee email address, password or customer database has been compromised the instant it is posted on a chat room, website or message board. CyberAgent® proactively detects stolen personally identifiable information (PII) and compromised confidential data online. CyberAgent® is also the only identity monitoring solution designed for proactive cyber detection on an international level – breaking language barriers and detecting identity theft across the globe. This gives businesses the opportunity to react to the compromised information and subsequently mitigate the impact and risk of that stolen credential.

[4] www.nytimes.com/2013/01/01/technology/antivirus-makers-work-on-software-to-catch-malware-more-effectively.html?pagewanted=all&_r=0
[5] http://krebsonsecurity.com/2012/06/a-closer-look-recent-email-based-malware-attacks/
[6] How useful is antivirus software, *ComputerWorld*, June 23, 2012

The second component to Enterprise Threat Intelligence is monitoring for and identifying company devices with compromised IP addresses. Most malware does two things: collects information from the compromised device and then sends this information to a command and control center where it is stored until the hacker makes use of it. Via its Enterprise Threat Intelligence software, CSID can detect when an IP address associated with a company or a network makes an outward communication to a known command and control center.

CSID collects more than 76,000 new malware variants every single day. These variants are collected from numerous publication distribution points including Newsgroups, FTP, Infected websites and communities

Once these malware variants have been collected, they are scanned and analyzed to identify any locations they are communicating with, either sending stolen data back to or receiving additional instructions. CSID can then match up the IP address communicating with the command and control center against IP addresses from a company and identify compromised systems and types of data extracted from those systems. CSID's Enterprise Threat Intelligence technology identifies nearly eight million compromised IP addresses every 14 days.

The implications of IP address monitoring are substantial for cyber security. With IP address monitoring, compromised information can be identified and dealt with before it ends up on the Internet black market or before it can be used to delve deeper into a company's confidential files. With IP monitoring there are also no false positives – every single IP address identified in the system is connecting to and exchanging information with a command and control center that it shouldn't be connected to.

Businesses, no matter how large or how much money they invest in system security cannot keep up with the rate that malware is evolving. Enterprise Threat Intelligence, specifically IP address monitoring, directly addresses this problem by bypassing inherent problems with signature based monitoring, and instead focusing on identifying unwanted communications between an infected device and a command and control server. This method not only fills in the monitoring gaps inherent with signature based monitoring, but also allows for the quicker identification of compromised systems.

CSID's Enterprise Threat Intelligence technology identifies nearly 8M compromised IP addresses every 14 days

ABOUT CSID

CSID is the leading provider of global, enterprise-level identity protection and fraud detection technologies and solutions to the world's top companies and government organizations. With CSID's advanced enterprise-level solutions, businesses can take a proactive approach to protecting the identities of their consumers all around the world. Products go beyond credit monitoring and include full-service identity theft protection; insurance and restoration; identity authentication and voice biometrics; and proactive breach preparation from discovery to resolution. CSID is the leading provider of global, enterprise-level identity protection and fraud detection technologies and solutions. The company's technologies power more than 70 percent of the retail identity protection industry.

ABOUT ENTERPRISE THREAT INTELLIGENCE

Did you know that the most popular password in 2011 was "password"? Many individuals tie multiple elements of their lives to a single, easy-to-crack credential, unknowingly increasing the risk of data compromise for themselves and the enterprises they associate with. If another enterprise's database is hacked and your consumer's credentials are attached to it, your business is now opened up to a potential compromise as well. And in today's cyber landscape, there are countless ways that fraudsters can infiltrate your digital real estate, and it's happening all the time. Businesses should consider cyber attacks and data loss a statistical certainty and be prepared to mitigate the impact of this loss.

CSID's Enterprise Threat Intelligence service, led by CyberAgent®, enables a business to proactively watch for data compromise and in turn, prevent and mitigate the risk associated with data breach.

CONTACT

For more information about CSID's Enterprise Threat Intelligence technology, visit www.csid.com or email sales@csid.com.