

## **Malware as a Service**

**Andrew Price**

**Director, Product Management, XYPRO Technology Corporation**

December 2011

The cloud has spawned many types of services – Software as a Service (SaaS), Platform as a Service (PaaS), Infrastructure as a Service (IaaS), and others. Now add a new one. According to the 2011 Data Breach Investigations Report (DBIR),<sup>1</sup> recently published by Verizon, it's *Malware as a Service (MaaS)*.

Verizon's 2011 DBIR sends a clear message – small companies, watch out. The Internet has become a source of free or low-cost malware that is easily customizable to meet every hacker's needs. Malware as a Service significantly reduces the skill set needed by a cybercriminal to launch automated attacks. The result is a shift in the demographics of information-asset attacks from large corporations to smaller companies.

The DBIR suggests two reasons for this change in attack demographics – the success of law enforcement and the emergence of Malware as a Service. Law-enforcement successes are motivating cybercriminals to look for softer, less risky targets. Malware as a Service is making the effort of attacking smaller companies more attractive.

In this article, we look at the DBIR's path to these conclusions.

### **What is the DBIR?**

The 2011 DBIR is the seventh in a series of reports on data breaches investigated by Verizon. The number of Year 2010 breach incidents analyzed in this year's DBIR has been significantly expanded by breach data provided by the United States Secret Service. The USSS was formed in 1865 to combat counterfeiting of the newly issued U.S. paper currency. It is now charged with safeguarding payment and financial systems in the United States.

The DBIR analyzes breaches in terms of the number of breach incidents and the number of compromised records (a "record" is a card number, a file, or some other data unit). In 2010, the combined forensic databases of Verizon and the USSS held the details of 761 data-breach incidents.

### **2010 – Surprise!**

The results of the analysis of Year 2010 breaches provided quite a surprise. The number of compromised records dropped by two orders of magnitude from its peak just two years earlier!

---

<sup>1</sup> [http://www.verizonbusiness.com/resources/reports/rp\\_data-breach-investigations-report-2011\\_en\\_xg.pdf](http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf) .

After four years of increases, compromised records hit an all-time high of 361 million in 2008. In 2009, this number had dropped to 144 million compromised records. Clearly, something was changing. Was corporate security getting that much better?

Then in 2010, less than 4 million records were compromised. 361 million to 144 million to 4 million! Something significant was happening. Was it simply that fewer incidents were being investigated? No – there were 70% more incidents investigated in 2010 than in the previous years.

The clue to this drastic reduction was that the number of compromised records per incident from 2004 through 2009 averaged 2,000,000, but this statistic dropped drastically in 2010 to less than 7,000 records per incident. Even more telling is that in years prior to 2010, 13% of all breaches exceeded 1,000,000 records (mega-breaches). In 2010, 93% of all breaches compromised less than 10,000 records; and there were no mega-breaches.

Is this a trend or an anomaly? Unfortunately, as it turns out, this is an anomaly. Mega-breaches have returned in force in 2011, with Sony, Epsilon, RSA, Citigroup, and Steam being prime examples. Sony itself contributed more than 100 million records to the hackers. But this anomaly had a fortunate outcome. It exposed a much more subtle but equally serious threat – the commoditizing of malware to make it available to even inexperienced hackers. As the Verizon report indicates, companies not only must continue to protect themselves against mega-breaches but now must be able to detect and maintain a growing number of mini-breaches.

Let us first review the Verizon DBIR methodology in order to trace the DBIR findings to the new security threat – Malware as a Service.

## Verizon's Methodology

Verizon describes a breach incident as a series of events. If the event chain is broken, the breach might not occur.

Events are characterized by four attributes – the Four As:

- Agent: An entity that caused or contributed to the incident.
- Action: An action taken by an Agent.
- Asset: Which of the victim's assets were affected.
- Attribute: How the asset was affected.

The Four As form the *Verizon Enterprise Risk and Incidence Sharing* (VERIS) framework, into which each incident is analyzed and recorded.

### Agents

Verizon categorizes Agents into external and internal, and internal Agents into active and passive:

- An External Agent is a lone hacker or organized crime group outside of the organization.
- An Internal Active Agent is a manager, employee, or contractor who maliciously participates in a breach.
- An Internal Passive Agent is a person internal to the company who inadvertently participates in the incident due to some error.

92% of all incidents investigated in 2010 and 99% of all compromised data were attributed to External Agents. Over half of them were organized crime groups.

However, Internal Agents accounted for the majority of stolen company confidential information. In fact, most attacks by Internal Agents were active and malicious.

### **Actions**

Actions include:

- Malware – any software used for the purpose of compromising information assets.
- Hacking – an attempt to access or harm information assets.
- Physical – using physical devices to compromise data.
- Misuse – using trusted resources or privileges for unintended purposes.
- Social – intrusion by deception or bribery.
- Errors – anything done incorrectly or inadvertently.

Malware includes the installation of backdoors through which an attacker can gain access to a system; key loggers, frame grabbers, and RAM scrappers; and interference with security controls. Malware may be injected via emails or compromised web sites.

Hacking is any effort to access or harm information assets by thwarting security mechanisms. Hackers may gain entry to a system via a backdoor or via the use of stolen, guessable, or default login credentials.

Attaching skimmers to ATMs and pay-at-the-pump card readers and using hard drives to copy confidential data are examples of physical actions.

Skimming credit-card information and embezzlement are misuses of trusted assets. For instance, wait staff are entrusted with possession of credit cards while preparing bills.

Social actions may be collusion with bank tellers to steal account information or with wait staff to skim credit-card information. Deception is a common social action – for instance, sending a phishing email or pretexting to be a repair man in order to replace POS devices with compromised devices.

Errors include omissions, misconfigurations, programming errors, etc. A frequent example of an error is the failure to change default credentials.

Hacking and malware are by far the most common actions, each having been used in half of all incidents in 2010.

### **Assets**

Assets that were involved in the incidents studied in the 2011 DBIR include:

- Servers.
- User Devices
- Offline data
- People

Multiple assets were often attacked in an incident.

Servers were compromised in over half of all incidents by being infected with malware. POS servers, database servers, and web servers were compromised most often.

User devices also were involved in over half of all incidents. User devices include POS devices, ATMs, pay-at-the-pump terminals, laptops, and desktops. These devices are popular because they handle

financial transactions, and many are open to the public. Interestingly, smart phones and tablets did not play a role in any attacks – yet.

Offline data assets comprise confidential documents and removable media from which information is stolen. People may be deceived, bribed, or intimidated into participating in a breach action.

**Attributes**

Attributes pertain to the security of an information asset. A security incident negatively affects one or more attributes. Security attributes that were impacted by attacks studied in the DBIR include:

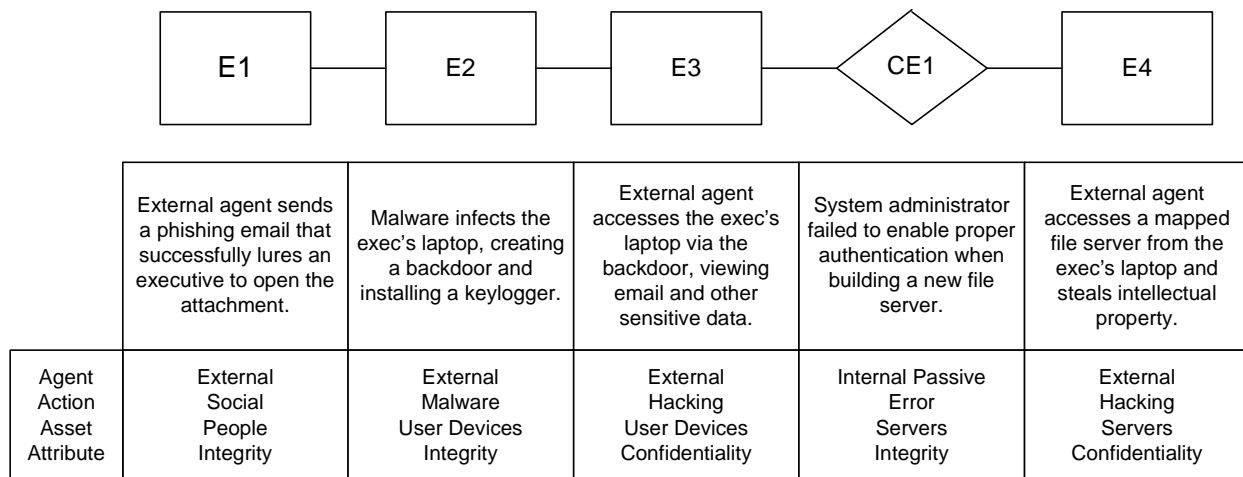
- Confidentiality –The information asset has limited access for observation and disclosure.
- Integrity – The information asset is complete and unchanged from its original state.
- Authenticity – The information asset is genuine and valid.
- Availability – The information asset is ready to use when needed.

Of course, all incidents compromise the confidentiality of the asset. Furthermore, most malware attacks compromise the integrity of the system since they modify the system to meet their needs.

An example of an authenticity impact is the swapping of a legitimate device for a phony one and initiating fraudulent transactions. Compromising the availability of an asset is not normally the purpose of an attack but is often collateral damage.

**An Example**

The following example of a breach incident is taken from the 2011 DBIR. It diagrams a chain of events that led to a successful breach. It shows four primary threat events (E1 through E4) and one conditional event (CE1) – an event not perpetrated by an attacker. The diagram gives a brief description of each event and the specific Four A attributes associated with each event.



**A VERIS Diagram of a Breach Incident**

If any of these events had been thwarted, the breach would not have occurred. One advantage of the VERIS diagram is that it is educational in terms of what could have been done to foil the breach. For instance, security awareness and email filtering could have prevented E1 from occurring. An antivirus product on the executive's laptop might have stopped E2. Stopping progression between E2 and E3

might have been accomplished if egress filtering or netflow analysis had detected the backdoor. Training and well-documented change-control procedures could have prevented the administrator's misconfiguration, described in the conditional event, and would have precluded the compromise of intellectual property in E4.

## **From Mega-Breaches to Mini-Breaches**

A striking observation from the 2011 DBIR is the absence in 2010 of mega-breaches of millions of records and the rapid increase in mini-breaches. As noted earlier, in the 2004 to 2009 timeframe, 13% of all breaches compromised more than one million records, with the average breach compromising two million records. In 2010, 93% of all breaches compromised less than 10,000 records and averaged less than 7,000 records per breach incident. There were no mega-breaches.

Verizon suggests two reasons for the change in breach strategy – the success of law enforcement and the emergence of Malware as a Service.

### Law Enforcement Successes – The Stick

The USSS has experienced significant success in fighting cybercrime. Over the last several years, USSS agents have arrested and prosecuted more than 1,200 suspects for cybercrime involving a total of over \$500 million in actual fraud loss. In addition, because of these arrests, the USSS estimates that it has prevented an additional \$7 billion in potential losses.

The perpetrators of many of the largest data breaches are now behind bars. After any major investigation that leads to the incarceration of big-time hackers, cybercriminals evaluate what happened; and their tactics evolve from the lessons learned. The main lesson learned from the law enforcement successes is perhaps that bigger isn't better. Mini-breaches attract less attention and therefore are less risky.

As a consequence, cybercriminals are now going after easier targets that provide a smaller but steady stream of compromised data and its resulting revenue. Though financial-service companies remain a major target for some cyber groups, these companies are no longer the predominant focus of cybercriminals. Rather, companies such as hotels, restaurants, and retail stores are becoming the predominant targets.

Going hand-in-hand with this modus operandi, the people behind breaches are no longer wholesalers stealing millions of credit-card numbers and selling them on the black market. Rather, they are using the fruits of their breaching activities for their own purposes. Cybercriminals are moving to compromised POS devices, fraudulent ATM withdrawals, account takeovers, and ACH transaction fraud.

### The Internet Comes to the Rescue of the Cybercriminals – The Carrot

Launching an effective attack on a well-protected company takes a lot of skill, time, and resources. Why go after small companies when the return can be so small?

Underground developers all over the world are making this attractive. A raft of prepackaged malware has recently become available on the Internet. Some is for sale; some is, in effect, open-source and free.

Many of these malware packages are customizable. They provide a basic backdoor or a basic keylogger, for instance, which can be modified to meet the hacker's specific needs through a GUI interface. Just a few clicks and the hacker has his chosen malware, customized to launch the specific attack he has in mind. Furthermore, if he is a serious and frequent hacker, he can modify his malware periodically to avoid detection by antivirus software.

Furthermore, there is a growing use of antforensic capabilities being included in the customizable malware. Techniques such as data-wiping (deleting evidence of an attack) and data-hiding (hiding or

obfuscating data via encryption or steganography) are making commodity malware harder to detect and harder to track back to the perpetrator.

Verizon found that the majority of highly automated attacks against small organizations in 2010 used customized malware. The cost of launching such attacks is low, and the skill requirements are becoming minimal. The technology is growing ever more accessible to an increasing number of criminals. Verizon's data shows that the requirement for a high skill level for successful attacks dropped from 90% of all incidents in prior years to just 8% in 2010.

This is *Malware as a Service*. It is changing the face of automated attacks against secured information assets.

## **The New Demographics**

Several observations from the 2010 data support the fact that cybercriminals have moved from large, difficult targets to smaller, softer, less risky ones. Restaurants, hotels, and retail establishments accounted for 65% of all incidents. Over half of the successful attacks were against organizations with less than 100 employees.

Even more telling is the distribution of compromised records. In past years, over 90% of such records were stolen from financial firms. In 2010, this number dropped to 35% - an almost two-thirds reduction. 56% of compromised records came from retail stores, hotels, and restaurants.

Several other statistics in the 2011 DBIR also point to the supposition that it is the smaller firms that are experiencing attacks. Large firms have typically implemented sophisticated security measures for detecting and containing data breaches, Not so, evidently, for small firms, as is shown by how they discovered the breaches, how long it took them to discover the breaches, and how unsophisticated they were in their security defenses.

### ***Breach Discovery***

The smaller firms were not proactive in discovering breaches. In fact, they often did not discover breaches at all. In 86% of the incidents, it was some third party that discovered the breach and reported it to the company. Third parties included customers, partners, and law enforcement agencies. Many of the breaches were discovered by banks and credit-card companies using CPP (Common Point of Purchase) investigations, which identify suspected fraud based on the purchase histories of stolen cards and account numbers.

5% of all breaches were reported by employees who saw odd things happening.

Only 6% of breaches were discovered by a process specifically designed for breach detection, such as logging to a SIEM (Security Information and Event Management) system. Tragically, Verizon's forensic analyses discovered that 69% of all breaches were detectable from data contained in a company's system logs. Clearly, most of the breached companies had no capability to make effective use of their log information on a timely basis.

Verizon notes that how victim companies discover a breach is an indicator of how well they know and monitor their own environments. An effective way to contain a breach is to consolidate log activity in a SIEM and to use a log-analysis tool to rapidly detect suspected intrusions. If all breached companies had adopted this technology, the number of breaches could have been reduced by a factor of two-thirds!

### ***Timespan***

Good security measures should quickly detect and contain a security breach. Verizon defines three time phases for breach containment:

- Compromise – The time from point of entry to the actual data compromise.
- Discovery – The time from the data compromise to the discovery that there has been a breach.
- Containment – The time from the discovery of the breach to the containment of its effects.

Interestingly, over half of all attacks took days or more to reach the point of compromise. This time period is the window of opportunity for a company to detect an intrusion and to stop it. Clearly, even several days was not enough for many small companies to notice an attack in progress.

Once a company's data had been compromised, three-quarters of the companies took weeks to months to discover the breach. This is perhaps explained by the fact that many of these companies were notified as a result of a CPP investigation, which can take this long. Less than 5% of companies discovered the compromise within hours of its occurrence. These were probably the larger companies with sophisticated security protections in place.

After an intrusion was discovered, it took two-thirds of the companies weeks to months to contain the intrusion. This has to be particularly frustrating to a company when it knows that its data is being stolen but is unable to stop the attack.

These timelines point out that smaller companies not only are not using good security protection methods, but that they also have neither an incident plan nor an incident staff in place. How can a store or a hotel afford this? No wonder they are the soft targets after which cybercriminals are now going.

### **PCI DSS Compliance**

Many of the victim companies were required to be PCI DSS (Payment Card Industry Data Security Standard) compliant. How did the small companies that were the targets of these attacks fare in this regard?

Not well. 89% of the victim companies had not validated their compliance within the last twelve months, as required by the standard. Most companies encrypted data at rest and in transit because these are capabilities supplied by their equipment vendors. However, they were noncompliant in the following areas. They failed to:

- Monitor access to network resources and cardholder data (89%)
- Maintain an information security policy (84%)
- Install and maintain a firewall to protect data (82%)
- Maintain secure systems and applications (81%)
- Regularly test security systems and processes (81%)
- Protect stored data (79%)
- Assign a unique ID to each person with computer access (74%)
- Change vendor-supplied password defaults (67%)

Sadly, monitoring access to network resources and cardholder data, coupled with a strong firewall, is the best defense against backdoor attacks, which accounted for a good many of the successful breaches.

### **Verizon's Recommendations**

Verizon ends its report with several recommendations for best security practices, many of which are particularly relevant to small organizations. As might be expected, the recommendations do not depart very much from Verizon's previous reports. The recommendations include:

- Identify and implement the essential security controls first, and then move on to more advanced controls where needed. Make sure that the basic protection infrastructure is in place.
- Be sure to always change default credentials, and ensure that passwords are not shared among users or among systems.
- Confirm that active accounts are valid, necessary, and have been given the minimum set of required privileges. Deprovision user access and privileges when no longer needed.
- Restrict and monitor privileged users.
- Secure remote access services, especially those that are Internet-facing. Restrict access to sensitive systems within the network.
- Monitor and filter outgoing traffic.
- Perform code reviews of new applications or modifications. SQL injection, cross-site scripting, authentication bypass, and exploitation of session variables played a role in half of the breaches.
- Enable logs, and monitor them. Often, information about a breach was available in the logs; but no one noticed.
- Shift focus from real-time detection to “this-week” detection.
- Increase awareness of social engineering, including fraudulent links, suspicious email, suspicious sites, and pretexting.
- Look for signs of tampering with physical devices such as ATMs and pay-at-the-pump devices.
- Create an incident-response plan.
- Engage in mock incident training.

Other recommendations based on XYPRO’s experience are:

- Use SSL and file-encryption solutions when possible.
- Ensure that platforms and applications that receive sensitive information also protect it.
- Ensure that administrators of other platforms and applications receiving your data do the same.
- Put granular auditing and access control in place.
- Feed audit data into a SIEM device to get an enterprise-wide view of security events.

Verizon has made the VERIS framework available to any company, and it encourages all companies to share their breach experiences so that all may learn and improve their defenses against information-asset attacks.

## Summary

The Verizon 2011 DBIR demonstrates that small companies must become more proficient in the protection of their information assets. Cybercriminals are moving away from the difficult, high-risk targets such as financial-service organizations and are instead focusing their efforts on softer targets that require less skill and that are of less interest to law enforcement.

This move is being propelled forward by the prolific availability on the Internet of sophisticated malware of all types. These products not only are easily customizable, but they also are increasingly using powerful antiforensic techniques to prevent their detection and to hinder the determination of the source of the attacks. With this malware, data theft is no longer the province of the skilled few. It is becoming available to the nefarious masses.

The absence of mega-breaches seems to have been an anomaly in 2010. 2011 already has experienced its share of targeted mega-breaches, including Sony, Epsilon, RSA, Steam, and Citigroup. Companies must continue their efforts to protect against these mega-breaches. Nevertheless, Malware as a Service is moving the focus of good security practices into the little companies that right now are ill-prepared to provide good security controls. Verizon estimates that 96% of all breaches were avoidable without difficult or expensive corrective action. 69% were detectable from the system logs. It seems that a little education will go a long way to combat the ill effects of Malware as a Service.

*Andrew Price is Director of Product Management at XYPRO and has over 21 years' experience in the mission-critical IT industry. Prior to joining XYPRO, Andrew was with ACI Worldwide for over 11 years, where he held roles in Product Management, Development and Architecture. Before ACI, Andrew worked as an applications development consultant to various NonStop users in Australia, North America, and Europe.*

*XYPRO Technology Corporation ([www.xypro.com](http://www.xypro.com)) has specialized in HP NonStop security software for nearly thirty years. XYPRO provides its XYGATE tools to achieve security compliance in HP NonStop environments in order to thwart security breaches such as those described in the Verizon DBIR. XYGATE security solutions range from Access Control, User Authorization, User Authentication and Password Quality to Automated Compliance, Audit Reporting, Integrity Checking, and FIPS 140-2 Validated Encryption. With respect to breach detection, as described in this report, XYPRO's Merged Audit product could have significantly reduced the number of successful intrusions.*