Technology Director Meeting

EDUCATION SERVICE CENTER, REGION 20

Serving the Educational Community

ESC★20
Serving the Educational Community

Mission: ESC-20 positively impacts the learning community **through high quality, cost effective products and services.**

Vision: To be the **definitive choice** for **leadership, innovation,** and the **advancement of learning.**

We believe...

in **service** first • **change is opportunity** • our employees **drive our success** • in **cultivating strengths** **collaboration** maximizes results • **learning** is **life-long** • in **purposeful** and **effective communication**

Strategic Drivers

Customer Service:
Create a service culture through a focus on the total customer experience.

Customer Focus: Listen to our customers, anticipate their needs, and create value that exceeds their expectations.

Employee Talent: Attract, grow, and retain top talent.

Continuous Improvement:
Create a culture of excellence through a mindset of continuous improvement.

Quality Objectives

Positive Impact on Education

Customer Satisfaction

Employee Satisfaction

Operational Excellence

Public Awareness/Relations

Strategies

Build relationships and **engage stakeholders**

Provide comprehensive **school improvement services** and **support**

Recruit and retain **high quality workforce**

Allocate resources to **develop** and sustain **quality products** and **services**

Implement a **performance excellence management system**

Agenda

ESC 20 Serving the Educational Community

- 2018 Verizon Data Breach Investigations Report
- Threat Intelligence
- Cyber Alerts – Spread the word!

Verizon Data Breach Investigation Report

"22 Instances of W-2 Scams in the education sector".

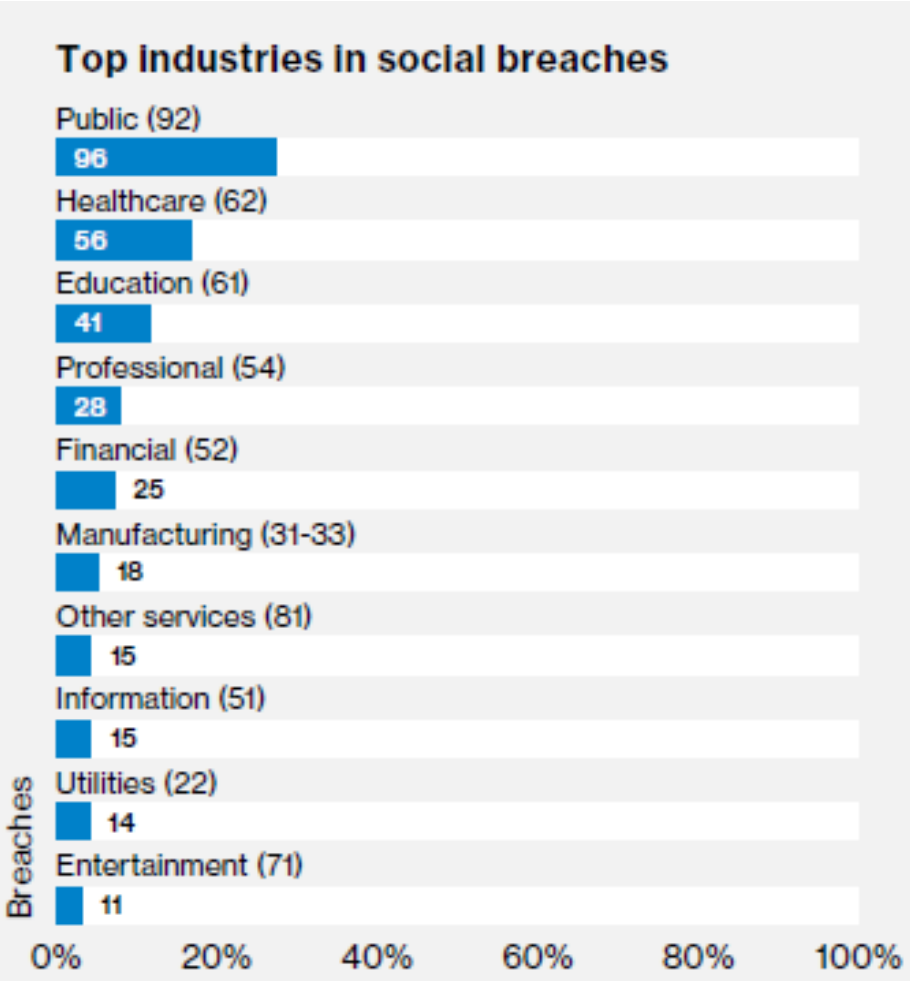


Figure 11. Top industries within Social breaches (n=351)

"It is not immediately clear why this scenario has figured so prominently in Education, but it may be due to the more "open source" nature of schools and universities".

"Denial of Service attacks remain extremely common in Education, and Cyber-espionage is still a significant pattern".

"Hacking and Social Engineering were the two most common types of actions against education".

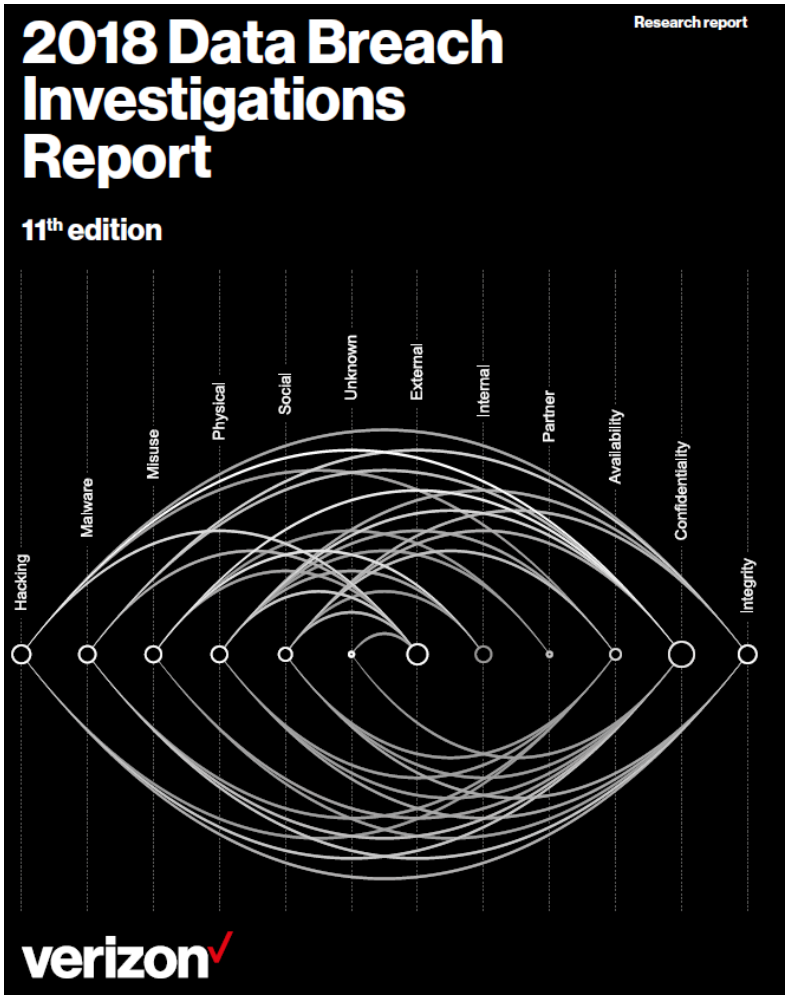
Verizon Data Breach Investigation Report

Things to consider:

1. Expect to be the target of a DoS attack.
    - What will be your response?
    - Review provider agreements.

2. Education - Mitigate human error by:
    - Performing regular security training.
    - Routinely audit configurations and processes.

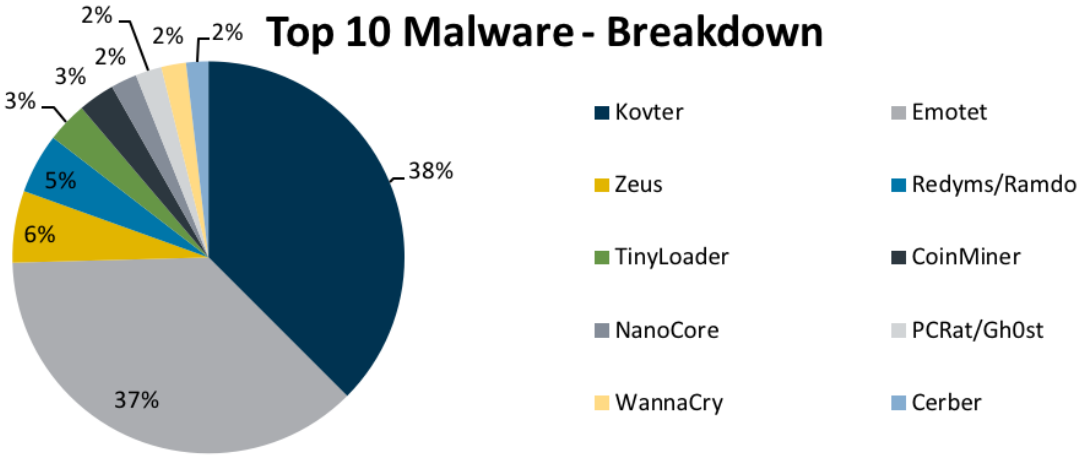
3. Make sure software is current.

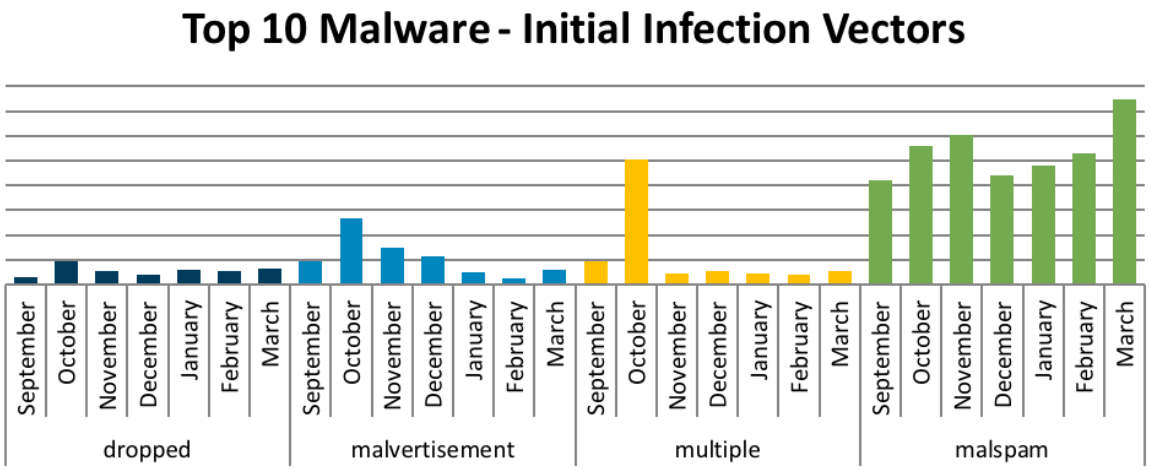


Google: 2018 verizon dbir

URL:
https://www.verizonenterprise.com/verizon-insights-lab/dbir/

Threat Intelligence





The MS-ISAC Top 10 Malware refers to the top 10 new actionable event notifications of non-generic malware signatures sent out by the MS-ISAC Security Operations Center (SOC).

Threat Intelligence

Malware Analysis Report

- The United States Computer Emergency Readiness Team (US-CERT) and the National Cybersecurity and Communications Integration Center (NCCIC) have provided descriptions and indicator information regarding submissions of malicious files.

Malware IPs and Domains Spreadsheet

- This list is produced from data collected by MS-ISAC. Currently, this data is being collected across a number of States and Local Governments. If you are using this information in your network security devices, MS-ISAC recommends reviewing and removing old indicators from previous lists as they are no longer being logged by the MS-ISAC and may no longer be malicious.

Cyber Alerts – Spread the Word!

- ESC-20 Technology Alerts Page
  https://www.esc20.net/page/it_ins.techdirinfo.alerts

- Multi-State Information Sharing & Analysis Center (MS-ISAC) Advisories
- SANS - Security Awareness Tip of the Day
- Security Tracker Vulnerability Summaries
- US-CERT – Alerts, Bulletins, Tips, Technical Documents

Thank You!

- If I was a bad guy, *what would I want* and *how would I get it*?
- Common sense is relative, *develop security sense*.
- *Plan to be impacted* by an incident.

Can you spot the hacker?

MS-ISAC Top 10 Malware Variants for March 2018

ESC★20
Serving the Educational Community

1. **Kovter** is a Trojan, which has been observed acting as click fraud malware or a ransomware downloader. It is disseminated via malspam email attachments containing malicious office macros. Kovter is fileless malware that evades detection by hiding in registry keys. Some reports indicate that Kovter infections have received updated instructions from command and control infrastructure to serve as a remote access backdoor.
2. **Emotet** is a modular Trojan that downloads or drops banking Trojans. Initial infection occurs via malspam emails that contain malicious download links, a PDF with embedded links, or a macro-enabled Word attachment. Emotet incorporates spreader modules in order to propagate throughout a network. Emotet is known to download/drop the Pinkslipbot and Dridex banking Trojans. Currently, there are four known spreader modules: Outlook scraper, WebBrowserPassView, Mail PassView, and a credential enumerator.
3. **ZeuS/Zbot** is a modular banking Trojan which uses keystroke logging to compromise victim credentials when the user visits a banking website. Since the release of the ZeuS/Zbot source code in 2011, many other malware variants have adopted parts of its codebase, which means that events classified as ZeuS/Zbot may actually be other malware using parts of the ZeuS/Zbot code.
4. **Redyms** is a click-fraud trojan that is primarily downloaded and dropped via exploit kit. Redyms has virtualization and sandbox detection and is primarily distributed in the United States.
5. **TinyLoader** is a backdoor trojan that is known for delivering point-of-sale and banking trojans, and is delivered via malvertising.
6. **CoinMiner** is a cryptocurrency miner that was initially disseminated via malvertising. Once a machine is infected, CoinMiner uses Windows Management Instrument (WMI) and EternalBlue to exploit SMB and spread across a network. CoinMiner uses the WMI Standard Event Consumer scripting to execute scripts for persistence.
7. **Gh0st** is a Remote Access Trojan (RAT) used to control infected endpoints. Gh0st is dropped by other malware to create a backdoor into a device, allowing an attacker to fully control the infected device
8. **NanoCore** is a RAT spread via malspam as a malicious Excel XLS spreadsheet. As a RAT, NanoCore can accept commands to download and execute files, visit websites, and add registry keys for persistence.
9. **WannaCry** is a ransomware worm that uses the EternalBlue exploit to spread. Version 1.0 is known to have a "killswitch" domain, which stops the encryption process. Later versions are not known to have a "killswitch" domain. WannaCry is disseminated via malspam.
10. **Cerber** is an evasive ransomware that is capable of encrypting files in offline mode and is known for fully renaming files and appending them with a random extension. There are currently 7 versions of Cerber and it has evolved specifically to evade detection by machine learning algorithms. Currently, v1 is the only version of Cerber for which a decryptor tool is available.

Verizon Data Breach Investigation Report

"Denial of Service attacks remain extremely common in Education, and Cyber-espionage is still a significant pattern".

Patterns in Education

Frequency	292 incidents, 101 with confirmed data disclosure
Top 3 patterns	Everything Else, Web Application Attacks and Miscellaneous Errors represent 76% of breaches
Threat actors	External (81%), Internal (19%), Partner (2%), Multiple parties (2%) (breaches)
Actor motives	Financial (70%), Espionage (20%), Fun (11%)
Data compromised	72% Personal, 14% Secrets and 11% Medical

Hacking and Social Engineering were the 2 most common types of actions against education.

- Social – 16% of incidents, 41% of breaches.
- Hacking – 72% of incidents, 44 % of breaches

Miscellaneous Errors

Incidents in which unintentional actions directly compromised an attribute of a security asset.

Notable findings
Over half of the breaches in this pattern were attributable to misdelivery of information – the sending of data to the wrong recipient. Misconfigurations, notably unsecured databases, as well as publishing errors were also prevalent.

Web Application Attacks

Any incident in which a web application was the vector of attack. This includes exploits of code-level vulnerabilities in the application as well as thwarting authentication mechanisms.

Notable findings
The number of breaches in this pattern are reduced due to the filtering of botnet-related attacks on web applications using credentials stolen from customer-owned devices. Use of stolen credentials is still the top variety of hacking in breaches involving web applications, followed by SQLi.