
2019
INCIDENT RESPONSE
How Hackers Attack
AVALONCyber

AVALONCyber

INCIDENT RESPONSE
How Hackers Attack

60% of SMB's will be out of business within 6 months of the event

THE CYBER THREAT IS REAL

Companies continue to fall victim to vicious cyberattacks. We all see it in the news and on social media, and our cyber team witnesses it daily. We often read that, no matter how much money they spend on their information security programs, large companies and organizations are still experiencing breaches. What we don't see or hear about in the news are the small to mid-size companies (SMBs) that are also under attack. And, unfortunately, many SMBs don't have the resources to bounce back—60% of them will be out of business within 6 months of the event, according to the National Cyber Security Alliance.

The problem is, most small business owners don't know they're a target and are, therefore, ill-prepared to safeguard against an attack. A survey published by Manta[1] shows that 87% of small business owners do not feel that they're at risk of a cybersecurity attack, and one in three small businesses don't have the tools in place—firewalls, antivirus software, network security monitoring, spam filters, data-encryption tools—to protect themselves. Some of these small businesses don't have an IT person, let alone a dedicated information security professional.

Over the past 12 months, Avalon Cyber was engaged in an extensive amount of incident response investigations on behalf of counsel representing businesses experiencing a security incident. Our core objective in these forensic investigations was to answer three primary questions for the client:

1. How did the adversary get into the network?
2. Where did the adversary go on the network?
3. What did they access and/or take?

The investigations spanned across different industries and involved different types of incidents—namely, ransomware, business email compromise, misconfiguration/human error, and hacking.

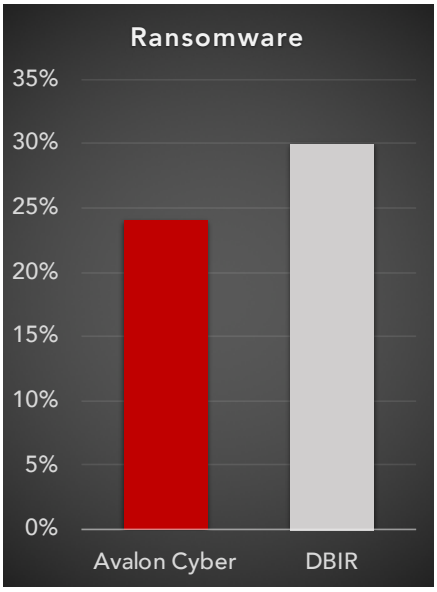
RANSOMWARE

This year, a ransomware attack will occur every 14 seconds, and by 2021, it will be every 11 seconds[2]. There were 850 million ransomware infections reported in 2018 alone. At Avalon Cyber,

[1] https://www.manta.com/resources/small-business-trends/small-business-owners-protecting-cyber-attack/?dest=%2Fresources%2Fsmall-business-trends%2Fsmall-business-owners-protecting-cyber-attack%2F
[2] https://phoenixnap.com/blog/ransomware-statistics-facts

AVALON Cyber

INCIDENT RESPONSE
How Hackers Attack



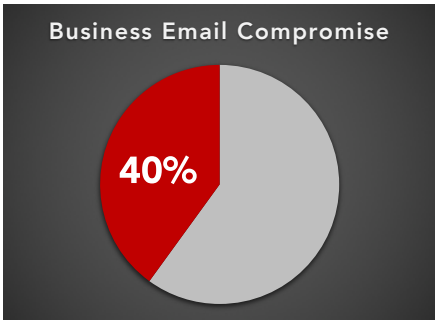
24% of our incident response investigations were in response to ransomware attacks.

The 2018 Verizon Data Breach Investigative Report (DBIR)[3] reported that 30% of the breaches that occurred involved malware or virus that would adversely affect an organization through extortion or ransomware attacks. That means that nearly 70% of the attacks that occurred were some other form of hacking, misconfiguration, errors or other means, which traditional antivirus products would never detect.

These attacks didn't appear to be directed at any particular industry but, in fact, affected healthcare, manufacturing, education, real estate, retail, professional services, and travel and tourism. In our investigations, we tried to determine if the incident was isolated to the ransomware event or if the adversary had infiltrated the network and accessed or exfiltrated any other protected data in the possession of the company. In 60% of our ransomware investigations, the event was a crime of opportunity for the adversary; in other words, the adversary had established persistency in the compromised corporate network and had obtained a foothold in the victim network weeks, if not months, prior to the detonation of the ransomware malware.

While some of these investigations did not prove, with a high degree of forensic certainty, that the adversary had accessed or exfiltrated other protected data from the business, they did show that they had a significant level of sophistication in their attack narrative and established a firm foothold in the victim network prior to discovery of the ransomware event.

24% of our incident response investigations were in response to ransomware attacks



BUSINESS EMAIL COMPROMISE

In November of 2009, the FBI put out one of their first warnings concerning spear phishing emails with malicious payloads. Since then, they have updated their annual reporting on this scheme with alarming statistics. In 2018, they reported that business email compromise (BEC) fraud is costing companies $12 billion dollars a year.

Approximately 40% of Avalon Cyber's recent cases involved a BEC attack. While the majority of these cases were in the real estate

[3] https://enterprise.verizon.com/resources/reports/dbir/

AVALONCyber

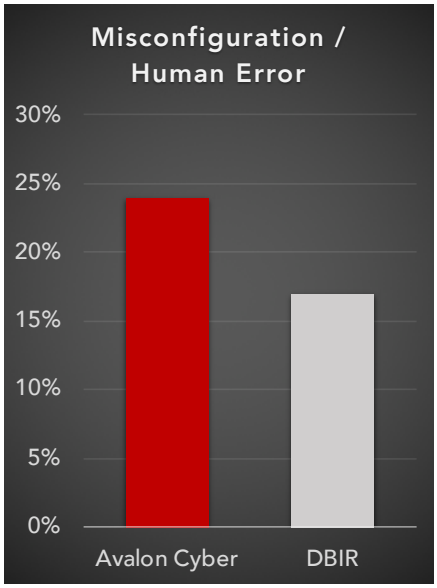
INCIDENT RESPONSE
How Hackers Attack

During our investigations of BEC cases, the companies suffered between $150,000 to $2.2 million dollars in unauthorized wire transfers

sector, which the FBI reports is the main target for this type of scam[4], several were also in the retail, manufacturing, and legal industries. In fact, Avalon Cyber experts have seen a major uptick in email compromises within the law firm and legal communities over the past 12 months.

The attack narrative was virtually the same in each of these cases. An end user of the organization (typically a targeted accounts receivable clerk or comptroller in the accounting department) received a phishing email and downloaded a malicious attachment or clicked on a link that redirected them to a bogus website, and thus, their credentials were compromised. Once the adversary obtained those credentials, they were able to log into the companies' Office 365 email systems and read through emails from vendors, suppliers, and customers. They then set up rules within Office 365 to hide all of the email correspondence between the accounting representative's compromised email account and the vendor requesting that all wire payments be directed to a new bank account.

The effects of a business email compromise like this can mean financial ruin for most companies. During our investigations of BEC cases, the companies suffered between $150,000 to $2.2 million dollars in unauthorized wire transfers in a matter of days or weeks.



MISCONFIGURATION/HUMAN ERROR

The Verizon 2018 Data Breach Investigations Report states that 17% of breaches studied in that report were caused by human error or misconfiguration of systems or user permissions.

Avalon Cyber investigation report data reveals that approximately 24% of our investigations were the result of error or misconfiguration. Two thirds of those cases involved the misconfiguration of a corporate website that allowed end users to access protected data behind a user name and password authentication page. It makes great business sense to allow customers access to information through the web, however, great care needs to be taken to ensure that the proper security measures and protocols are in place to protect against the unauthorized access of this information by adversaries.

[4] https://www.sosdailynews.com/news.jspx?articleid=5953CCEE3D35EFA0ACA3AA7429761CA0

AVALONCyber

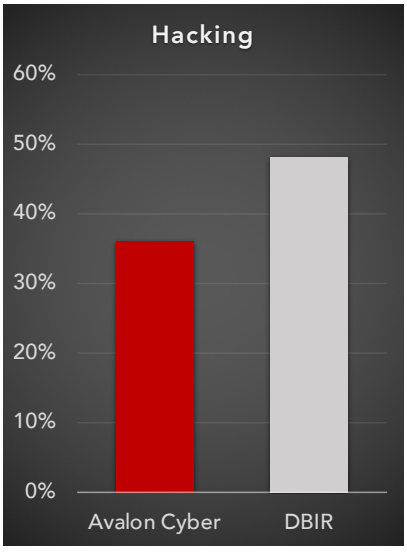
INCIDENT RESPONSE
How Hackers Attack

36% of Avalon Cyber incident response investigations, hacking was the root cause of the attack

As humans, we're apt to make mistakes, which is why you should automate any system that can be automated. If a regular setup procedure is performed often, it's better to make sure it is secure once and then just repeat it. Third-party security teams can perform security scans and/or audits regularly to discover future misconfigurations. These teams configure systems with the thought in mind that the system will get compromised because that is very likely. In case of a security breach, an attacker should only be able to do very little damage[5].

In addition to the misconfiguration errors we saw, some of the investigations involved incidents that were the result of preventable human error.

For example, a healthcare provider that inadvertently attached a spreadsheet with patient record information to an email instead of the intended letter to the patients advising them about a change in insurance coverage.



Another example involved an employee of a health insurance company who took a photograph of another employee and posted it on Facebook. The photo not only showed the happy employee, but her monitor in the background that contained clearly visible patient record information. Even careless human errors like these are reportable data breach events that still cost money to report and remediate.

HACKING

According to the DBIR, hacking as an attack vector makes up 48% of the breaches from 2018. Computer hacking refers to the practice of modifying or altering computer software and hardware to accomplish a goal that is considered to be outside of the creator's original objective. The majority of hackers possess an advanced understanding of computer technology. The typical computer hacker is an expert in a particular computer program and will have advanced abilities in computer programming[6].

In 36% of Avalon Cyber incident response investigations, hacking was the root cause of the attack and the vector by which the adversary gained initial access to the corporate network. The industries affected by hacking included education, retail, and manufacturing.

[5] https://blog.detectify.com/2016/06/17/owasp-top-10-security-misconfiguration-5/
[6] https://cyber.laws.com/hacking

AVALON Cyber

INCIDENT RESPONSE
How Hackers Attack

Unfortunately, traditional antivirus products are ill-equipped to identify or detect advanced hacking techniques because the adversary has mastered the ability to use existing Windows applications and software to escalate their permissions and move laterally within the victim environment without being detected. The applications and software they exploit are standard Windows systems programs that come with every Windows installation and are trusted applications within every antivirus product. This affords the adversary the cover of being able to establish a foothold in the victim environment and remain undetected for weeks, if not months, before being discovered.

ABOUT AVALON CYBER

Avalon Cyber experts have seen firsthand how hackers operate and know how to minimize your risk of a data breach. Avalon has decades of experience in digital forensics, cybersecurity incident response, IT risk management, law enforcement, and enterprise information security leadership. Avalon's experience spans commercial and government organizations including financial services, legal, healthcare, manufacturing, telecommunications, and more.

Our experts have or previously have held, top secret government clearances and possess key industry certifications including: CISSP, CISM, CISA, CRISC, CCNA, CCE, CFCE, EnCE, ACE. Our team was built on principles and sound ethics acquired over decades of law enforcement experience that can be relied upon and trusted.

To learn more about Avalon Cyber, visit:
www.avaloncybersecurity.com

For questions, please contact:
Ian Gattie
Director of Marketing
716.995.7777
ian.gattie@teamavalon.com