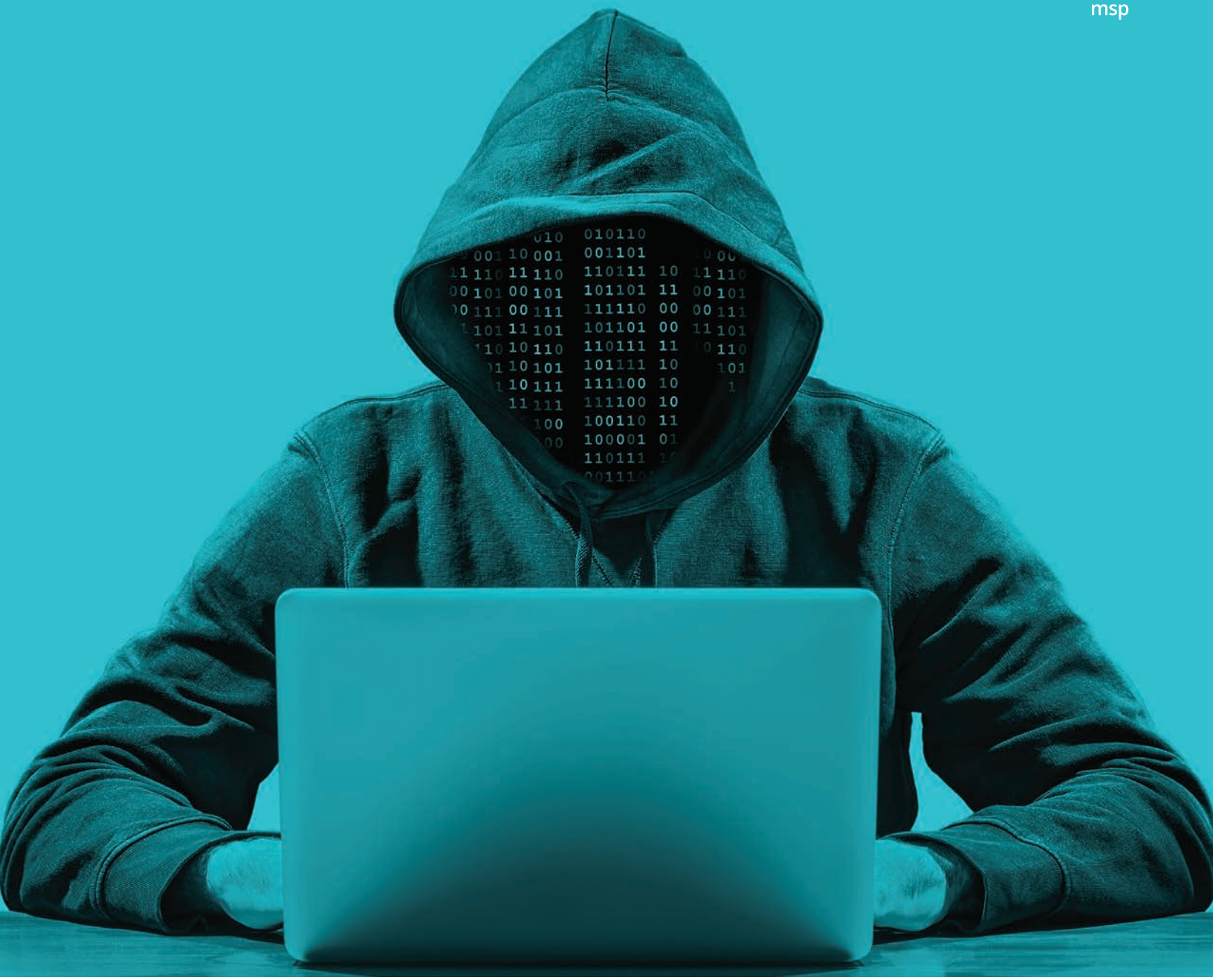
solarwinds msp



eBOOK

Think Like a Cybercriminal

INTRODUCTION

Cybercriminals are a diverse lot, yet you can spot some patterns and motives across the group. For victims, be they businesses or individuals, the outcome of an encounter can usually be quantified—some sort of loss has occurred. From here, you can start to understand the cybercriminal's motives. The degree of loss can suggest the motive and operating capability of the cybercriminal, but the type of attack must also be considered.

You can identify the operating capabilities of cybercriminals fairly easily—you simply need to answer the question, "How did the crime occur?" This information is readily available from security research firms—in some cases provided with excruciating technical detail—and the court documents from cybercriminals who have been brought to justice or indicted. But this is only half of the information we need to "think like a cybercriminal." The other piece of information is far more elusive—motivation.

If we want to understand the criminal mindset, then answering, "Why did the cybercrime occur?" might be more pertinent. In the examples we'll provide later, especially in the case of an "affiliated actor" (a group or organization that conducts a cybercrime and is known to the business or victim), the motivation can potentially be easily identified. In the cases of a "non-affiliated actor" (a group or organization that conducts a cybercrime and is unknown to the business or victim), the motivation for the cybercrime may be harder to pinpoint. In either case, we have to consider the result of the crime.

If the cyberattack results in monetary gain for the criminals, we can assume that the fraud, identity theft, extortion, blackmail, unauthorized financial transactions, or ransomware payload was perpetrated for profit. However, while many focus on the hacked party as the victim, few give any thought to the ultimate destination of the illicit gains. That money could end up going to fund a terrorist group (Cyber Caliphate), bypass currency controls for a sanctioned country (Lazarus Group), or bankroll a vast criminal enterprise (Carbanak group).

"You can identify the operating capabilities of cybercriminals fairly easily—you simply need to answer the question..."

In the case of a cyberattack conducted for the purposes of espionage or stealing intellectual property, the motivations of the cybercriminals could encompass a whole spectrum. These could range from advanced persistent threat (APT) groups known to be affiliated with the cyberwarfare capabilities of many nation states, or the cyberattack could be the result of third-party cybercriminal mercenaries hired by a rival organization. In the case of espionage and intellectual property theft, the potential motivations (and culprits) are vast.

There is, of course, a third type of cyberattack—an attack that seeks to damage, degrade, or destroy an organization and comes with no warning or demand from cybercriminals. From the victim's perspective, they are frequently not targeted for the attacks and are unfortunately part of the resulting collateral damage of a larger attack. WannaCry, NotPetya, and BadRabbit are examples of global cyberattacks that resulted in business losses. These occurred because of a self-propagating cyberweapon that led to a rapidly spreading cyberattack. Thus, there is the potential to be a victim from a random cybercrime as a cost of being online.

If there is such a thing as random cyberattack, there is of course the targeted cyberattack that has neither espionage nor a direct financial motivation. Affiliated actors, employees, or ex-employees can inflict grave harm on an organization.

In order to understand the cybercriminal mindset, it helps to break the attacks into two categories based on visibility, and then map them to the relationship of the actor to the victim's business.

CATEGORIES OF ATTACKS

High-Visibility Cyberattack—The resulting loss is clearly identified, and the attack is noisy. Ransomware deployments and distributed denial of service attacks are excellent examples.

Low-Visibility Cyberattack—The resulting loss is discovered over a period of weeks or months. The attack is stealthy, and the perpetrators make efforts to conceal their activities from the business. This is typically the domain of APT nation-state actors.

TYPES OF PERPETRATORS

Affiliated Actor—A group or organization that conducts a cybercrime and is known to the business or victim.

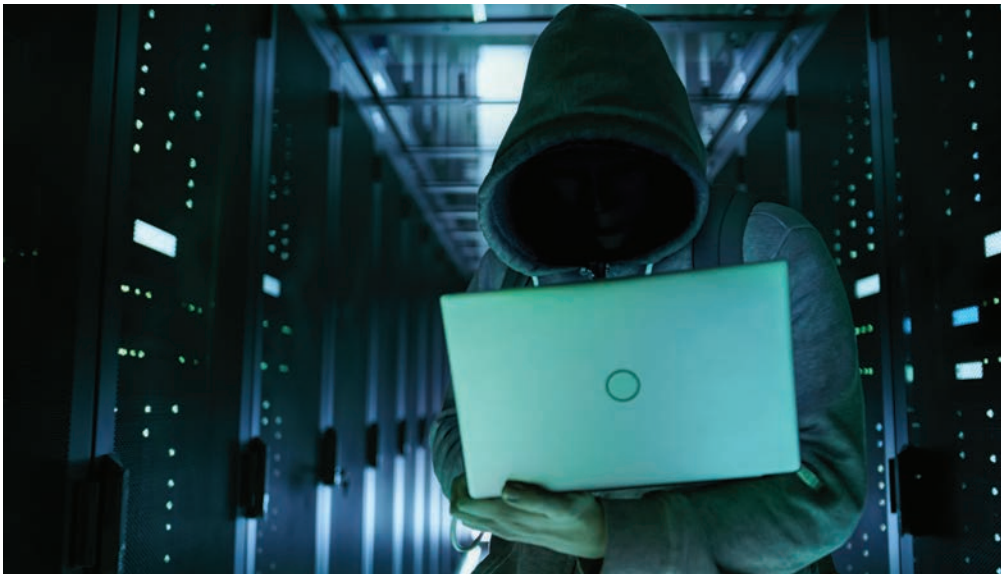
Unaffiliated Actor—A group or organization that conducts a cybercrime and is unknown to the business or victim.

HIGH-VISIBILITY CYBERATTACK—AFFILIATED ACTOR, ALSO KNOWN AS AN "INSIDER THREAT"

A malicious individual or group familiar with the IT systems of a business represents a serious threat. The effects of a high-visibility attack manifest fairly quickly, and the damage can be extensive. In the case of Christopher Gurpe, his methodical December 17, 2015 attack consisted of deleting configuration files, removing administrative-level accounts, and changing passwords on the switches of the core network[1]. His sabotage was conducted from a company asset, which he "wiped" before returning to his employer, Canadian Pacific Railway.

The damage estimate provided in the court documents was determined to be $30,000 in "lost business." However, given the critical nature of a rail transportation and logistics network, if an accident occurred—attributed fully or partially to his unauthorized access and sabotage—the liability could have reached millions of dollars in damages or fines.

Broadly speaking, the cause of an "insider" high-visibility attack is, at its core, a dispute or perceived indignity to the attacker perpetrated by the company or management. Examples include Dariusz J. Prugar, who systematically destroyed an Internet Service Provider and in part contributed to the company's demise, and James Cornish, an information technology employee at Shionogi who deleted virtual servers and hosts causing $800,000 in losses[2,3]. Both criminals used this common "dispute" theme to try to justify their actions. In the last two cases mentioned, almost no operational security was practiced before and during the cyberattacks. It is as if these individuals wanted to get caught for the ability to tell their story to a sentencing judge.



HIGH-VISIBILITY CYBERATTACK—UNAFFILIATED ACTOR

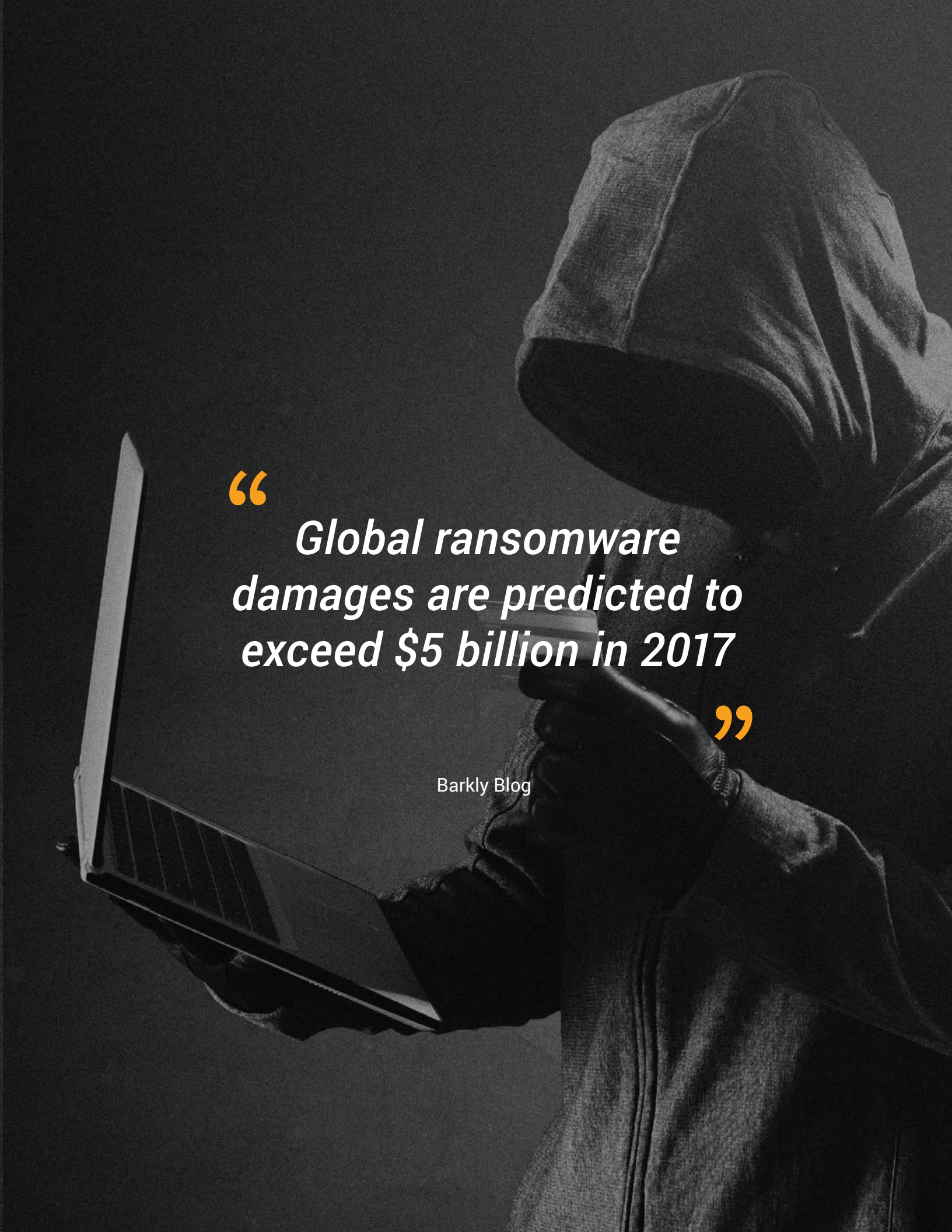
The information security press usually provides the details of how external data breaches or ransomware attacks transpire. This category of attack is by far the most likely to victimize a business. The latest numbers suggest 91% of cyberattacks and the resulting data breaches begin with a phishing email attack, and of those attacks, 93% of them are ransomware payloads[4,5].

In December of 2016, international law enforcement was compelled to act against the prolific spread of ransomware and banking Trojans. Operation Avalanche, as the operation was known, targeted infrastructure used to spread banking Trojans and many strains of ransomware.[6] The size and scope of the cybercriminal operation was revealed in many articles and press releases:

- 39 servers and hundreds of thousands of internet domains used by the Avalanche network—Europol[7]
- "40 different countries were involved and accused the network of hosting some of the world's most pernicious malware as well as several money laundering campaigns."—CBS® News, quoting the US Department of Justice[8]
- Five suspects in custody and several additional warrants issued—German Police[9]

Despite the best efforts of a continued and coordinated world-wide law enforcement effort, high-visibility ransomware attacks are growing at an alarming rate. Global ransomware damages are predicted to exceed $5 billion in 2017, according to an extensive and in-depth look at ransomware from the Barkly Blog[10].

91% of cyberattacks begin with a phishing email and 93% of them are ransomware payloads, according to a PhishMe report and the U.S. Department of Justice.


“
Global ransomware damages are predicted to exceed $5 billion in 2017
”
Barkly Blog

LOW-VISIBILITY CYBERATTACK—UNAFFILIATED ACTOR

Other cybercriminal tactics—where the motive is to extract money from businesses and individuals—do exist, but the methods vary across perpetrators, from malicious individual actors to fully structured cybercrime groups. According to the 2016 IC3 report, the strategy and capabilities cybercriminals employ include many low-tech and low-visibility tactics[12].

Chief among these tactics is the business email compromise (BEC), a cybercriminal attack that uses social engineering to yield the illicit transfer of funds. Arrests and prosecutions for the perpetrators of this type of attack have been frustratingly slow, given that IC3 statistics identify BEC in the number-one loss position, with a cybercrime payday of over £360 million in 2016—and over 12,000 US victims. With numbers like these, law enforcement engaged.

In March of 2017, a criminal complaint accused Evaldas Rimasauskas of perpetrating a massive $100 million fraud against Facebook® and Google®[13]. His attack? Incredibly simple. Register a company name, open a bank account closely resembling that of an Asian computer supplier, and send fabricated invoices to the victim companies. According to the indictment, it's believed his scam started in 2013 and carried on until detected in 2017.

This category of low-visibility cyberattacks includes APT actors. Although they employ many of the same techniques of financially motivated cybercriminals, the motivations of APT groups may be politically directed or focused on stealing intellectual property to advance a nation-state's agenda.

On October 23, 2017, the US Justice Department charged a 36-year-old Chinese national, Yu Pingan, also known as "GoldSun," with conspiring with two other Chinese nationals to hack the computer networks of the United States government computers at the US government's Office of Personnel Management (OPM) and those of a number of insurance companies, including Anthem®[14].

The criminal complaint identifies the use of a sophisticated malware tool called "Sakula," which was delivered to targeted endpoints by a compromised third-party website that victims visited frequently. This is known as a "waterhole attack." Yu Pingan used an Adobe® Flash® exploit and several zero-day exploits to attack any workstation that visited these compromised websites. On several occasions, intercepted communications warn him to "not draw the attention of the FBI."

Given the sophisticated tactics, tools, and procedures of the low-visibility attacks of an actor who wants to remain undetected in a successfully compromised network, the current state of detection provides a long period of time for the complete exploitation and exfiltration of information from that network. According to the 2016 Ponemon Institute Cost of Data Breach Study, "the mean time to identify this [type of] data breach is 201 days[15]."

LOW-VISIBILITY CYBERATTACK—AFFILIATED ACTOR

Low-visibility cybercrime by an employee or ex-employee is rare. With few high-profile cases to examine, they are rarely elevated to the public domain, yet they do happen. These sorts of cybercrimes are not massive, nor are they global in nature. They are typically related to disputes between developers of code and owners of code; sometimes these crimes extend to disputes over intellectual property.

One example of this sort of cybercrime is the allegations against Bo Zhang. The felony charges from 2012 allege Bo stole Federal Reserve Bank computer code, but the available information says little about what he did with that code after he stole it. What's interesting is that the code issue had little to do with his ultimate guilty plea. The press release and indictment allege far more serious crimes despite the $9.5 million spent "developing the code" for the Federal Reserve Bank. As the press release from the US Justice Department read:

During his guilty plea today, Zhang admitted that between 2011 and 2012, he submitted fraudulent documentation to immigration authorities to help foreign nationals obtain visas to enter and work in the United States. Zhang falsely represented to immigration authorities that certain foreign nationals worked full-time for his computer-training business. At least one individual fraudulently obtained a visa in connection with Zhang's offense[16].

During his guilty plea today, Zhang admitted that between 2011 and 2012, he submitted fraudulent documentation to immigration authorities to help foreign nationals obtain visas to enter and work in the United States.

The obscure and factually ambiguous story of Bo Zhang strikes a contrast with the legal saga of Sergey Aleynikov, who must once again defend the allegation that he stole high-speed trading code from Goldman Sachs® with the intention of bringing the code to a new startup[17]. Aleynikov's legal journey included a conviction, an appeal that overturned the conviction, and a recent appeal that reinstated the original conviction. With eight million dollars in legal bills and potentially four years in prison, Sergey faces an uncertain future.

UNDERSTANDING THE MOTIVES OF CYBERCRIMINALS

Examining the visibility of cyberattacks and the affiliation of the actors behind them can give insight into how the various types of cybercriminals think. These apply across tactics that range from the cyber "smash and grab" ransomware attacks to the most sophisticated and stealthy infiltration and exfiltration APT attacks. From the victim perspective, it really does not matter and the various laws are explicitly clear—the US Computer Fraud and Abuse Act (CFAA) and the UK Computer Misuse Act (CMA) use an all-encompassing term of "unauthorized access." Of course, there are a host of other laws applicable to illegal activity derived from cybercrime activities, such as blackmail, fraud, extortion, impersonation, cyberstalking, harassment, child exploitation, and a host of other internet and internet-facilitated crimes.

> "The single biggest existential threat that's out there, I think, is cyber."
>
> Retired US Admiral Michael Mullen

Retired US Admiral, Michael Mullen once asserted, "The single biggest existential threat that's out there, I think, is cyber[18]." Many feel this quote was overblown and represented a general angst about cyberattacks. However, the most important aspect of cybercrime is this—for every cyberattack, there is someone who can end up in handcuffs. Make sure to report all cybercrimes to help prevent future attacks and protect potential victims.

1. "Former Employee of Transcontinental Railroad Company Found Guilty of Damaging Ex-Employer's Computer Network," United States Department of Justice. https://www.justice.gov/usao-mn/pr/former-employee-transcontinental-railroad-company-found-guilty-damaging-ex-employer-s (accessed November 2017)
2. "New York Man Sentenced for Computer Hacking that Shut Down Internet Service Provider," US Department of Justice. https://www.justice.gov/usao-mdpa/pr/new-york-man-sentenced-computer-hacking-shut-down-internet-service-provider (accessed November 2017)
3. "Former Shionogi Employee Sentenced to Federal Prison for Hack Attack on Company Computer Servers," US Department of Justice. https://www.justice.gov/archive/usao/nj/Press/files/Cornish,%20Jason%20Sentencing%20News%20Release.html (accessed November 2017)
4. "Enterprise Phishing Susceptibility and Resliency Report," PhishMe. https://phishme.com/enterprise-phishing-susceptibility-report (accessed November 2017)
5. "2016 Q1 Malware Report," PhishMe. https://phishme.com/project/phishme-q1-2016-malware-review (accessed November 2017)
6. "Avalance Network Dismantled in International Cyber Operation," US Department of Justice. https://www.justice.gov/opa/pr/avalanche-network-dismantled-international-cyber-operation (accessed November 2017)
7. "'Avalanche' Network Dismantled in International Cyber Operation," Europol. https://www.europol.europa.eu/newsroom/news/%E2%80%98avalanche%E2%80%99-network-dismantled-in-international-cyber-operation (accessed November 2017)
8. "Police Make Arrests in 'Unprecedented' Cybercrime Crackdown," CBS News. https://www.cbsnews.com/news/cybercrime-takedown-police-make-arrests (accessed November 2017)
9. "Police Make 5 Arrests in 'Unprecedented" Cybercrime Takedown," The Enterprise. http://www.enterprisenews.com/news/20161201/police-make-5-arrests-in-unprecedented-cybercrime-takedown (accessed November 2017)
10. "Must-Know Ransomware Statistics 2017," Barkly. https://blog.barkly.com/ransomware-statistics-2017 (accessed November 2017).
11. "2016 Internet Crime Report," IC3. https://pdf.ic3.gov/2016_IC3Report.pdf (accessed November 2017)
12. "Lithuanian Man Arrested for Theft of Over $100 Million in Fraudulent Email Compromise Scheme Against Multinational Internet Companies," US Department of Justice. https://www.justice.gov/usao-sdny/pr/lithuanian-man-arrested-theft-over-100-million-fraudulent-email-compromise-scheme (accessed November 2017)
13. "United States of America v Yu Pingan," Politico. https://www.politico.com/f/?id=0000015e-161b-df04-a5df-963f36840001 (accessed November 2017)
14. "2016 Cost of Data Breach Study: Global Analysis," IBM and Ponemon Institute. https://www-01.ibm.com/marketing/iwm/dre/signup?source=mrs-form-1995&S_PKG=ov49542&ce=ISM0484&ct=SWG&cmp=IBMSocial&cm=h&cr=Security&ccy=US&&cm_mc_uid=17909256714515099347148&cm_mc_sid_50200000=1509934714&cm_mc_sid_52640000=1509934714 (accessed November 2017)
15. "Computer Programmer Pleads Guilty in Manhattan Federal Court to Stealing Proprietary Code from the Federal Reserve Bank of New York and to Engaging in Immigration Fraud," US Department of Justice. https://www.justice.gov/archive/usao/nys/pressreleases/May12/zhangboplea.html (accessed November 2017)
16. "Ex-Goldman Programmer's Code Theft Conviction Revived by New York Court," Reuters. https://www.reuters.com/article/goldman-sachs-aleynikov/ex-goldman-programmers-code-theft-conviction-revived-by-ny-court-idUSL1N1FE5OB (accessed November 2017)
17. "The Existential Angst of America's Top Generals," The FP Group. http://foreignpolicy.com/2015/08/04/the-existential-angst-of-americas-top-generals-threat-inflation-islamic-state (accessed November 2017)