F-Secure

INCIDENT RESPONSE REPORT

Introduction

Cyber attacks affect companies all over the world. Some attacks are relatively indiscriminate, such as the WannaCry ransomware attacks that swept the globe last spring.[1] Others are highly targeted acts of theft or espionage, such as 2016's attacks on the National Democratic Committee.[2] But all cyber attacks are a potential threat to the operations, reputation, and integrity of organizations.

When faced with a security incident, many companies opt to call in a team of incident response experts. These experts help organizations investigate the incident, mitigate the damages, and restore operations so they can get back to business as quickly and efficiently as possible. The following report is compiled from a random sample of past incident response investigations conducted by F-Secure's cyber security consultants. It contains insights into how adversaries breach networks, what tactics, techniques, and procedures (TTPs) they employ, and what they do once they breach security perimeters.

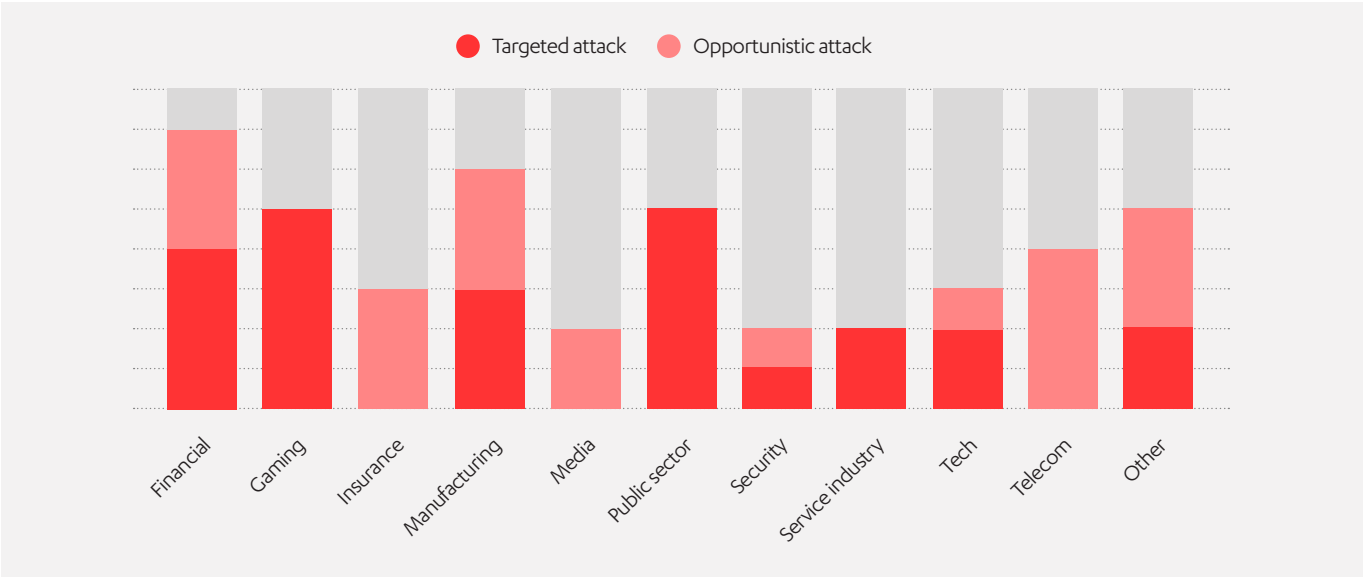
Investigations per industry

The above chart breaks down the data set used for this report by investigations per industry. The following observations will be most relevant to companies working in the finance, manufacturing, and telecommunication industries. But adversaries appropriate and repurpose TTPs to fit different needs and objectives, which produce clear patterns in how threat actors conduct attacks. Intelligence about these TTPs, how they are used, and for what purposes, will benefit organizations regardless of what business they're in.

Targets vs. opportunities

All cyber attacks can be broadly classified into one of two categories: opportunistic or targeted. Opportunistic attacks are situations where a threat actor attacks a target simply because an opportunity to do so presents itself. Targeted attacks involve a threat actor selecting a specific target and then using the necessary methods to compromise that target. Our investigations found that organizations experience security incidents from both approaches in approximately equal proportion to one another.

Targeted vs. opportunistic attacks



Targeted vs. opportunistic attacks by industry

But in our experience, there are some significant differences across industries. Gaming companies and public sector organizations, for example, seem to attract more interest from targeted attackers. In the data we reviewed for these two verticals, all investigations pointed to targeted attacks. On the other hand, the telecom and insurance companies included in our analysis were primarily affected by opportunistic attacks. It's also worth noting investigations conducted for financial organizations and manufacturers saw both approaches used in equal proportion to one another.

It is important to understand how methods differ between opportunistic and targeted attacks.

How attackers are getting in

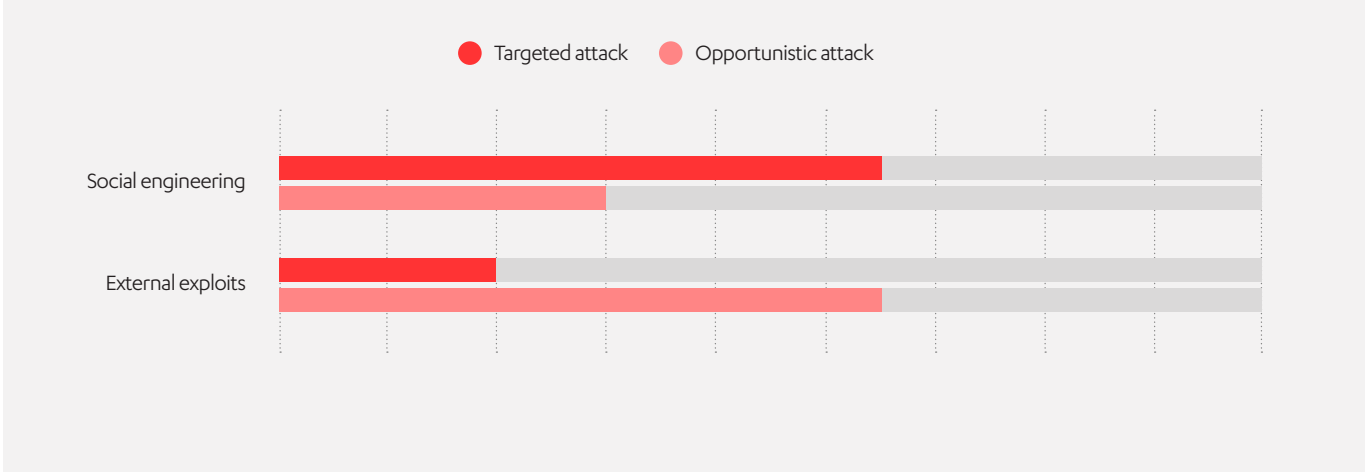
52%
Social engineering

48%
External exploit

Point of entry for external attacks

There are two potential weaknesses in organizations that adversaries try to exploit: people and technology.

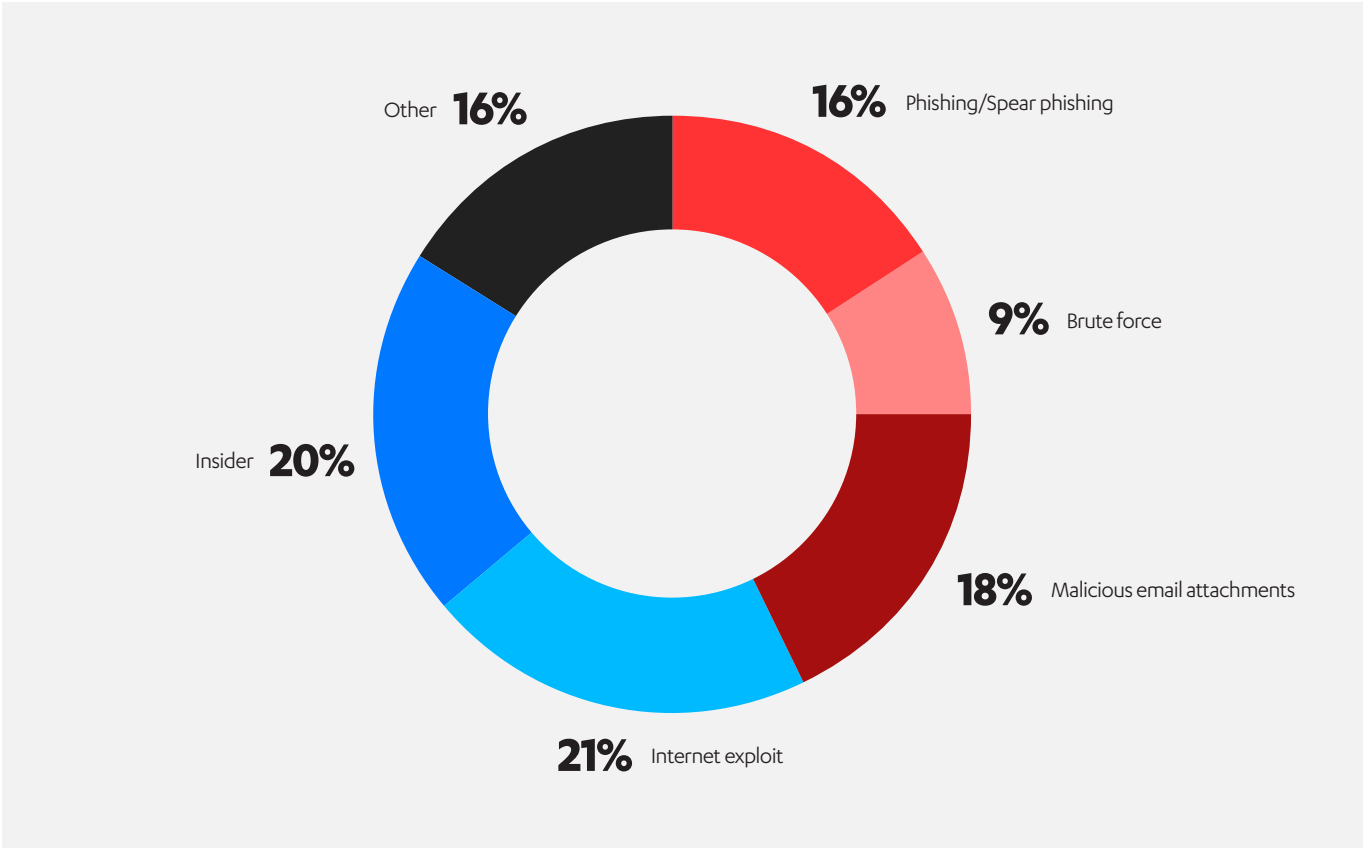
Adversaries exploit weaknesses in people through social engineering – manipulating victims into divulging information or performing actions that aid the attackers. Well-known examples include tricking victims into installing malware (via email attachments or web links) and fooling users into divulging credentials (via fake login pages). Social engineering was routinely used in the targeted attacks we analyzed.



Social engineering vs. external exploits in targeted and opportunistic attacks

Opportunistic attacks in the data relied more on technical weaknesses in an organization's IT infrastructure, such as exploiting software vulnerabilities.

Opportunistic attacks are often initiated with cost-effective target selection techniques, such as mass scanning the internet and attacking a vulnerable service when a new exploit comes out. This can be done in a matter of minutes using tools readily available on the internet. Targeted attacks select high value marks and then invest considerable time in learning about their intended victim to increase their chances of success. To put it simply: opportunistic attacks aim to hit many potential victims with cost-effective techniques, whereas targeted attacks focus their efforts on a limited number of high value objectives.

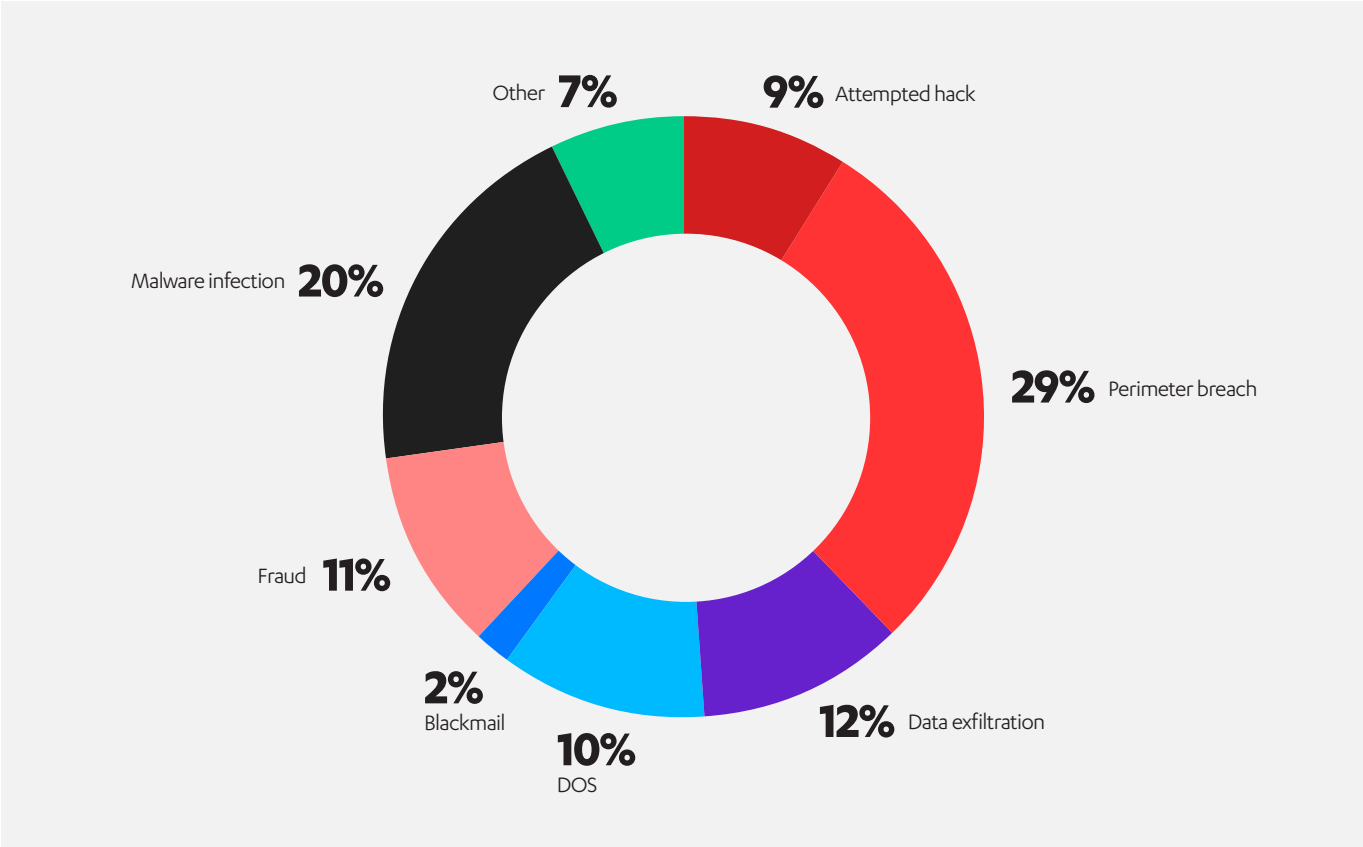


Type of attacks

Type of attacks

Insider threats (employees or trusted persons that attack the company from within) and internet exploits were the most common sources of compromise in the cases we studied. Internet exploits are attacks against a company's internet-facing infrastructure. These attacks involved a few different techniques, with the most common being an exploit against an unpatched vulnerability. These were particularly prominent in the weeks following the disclosure of a vulnerability/exploit in a popular piece of server-side software. Insider threats are defined as individuals trusted by an organization (such as an employee) who either on their own, or as part of a group, intentionally compromises the organization(s) that trusts them. In most of the insider threat cases we studied, insiders stole information (such as customer data or intellectual property) or conducted acts of industrial sabotage.

Phishing/spear-phishing and emails with malicious attachments were the next most common attacks seen in the data. Both types of attacks arrive in workers inboxes (phishing can also use messaging services or other platforms, but email is the most frequently used). It's important for organizations to be aware of this given email's widespread use.

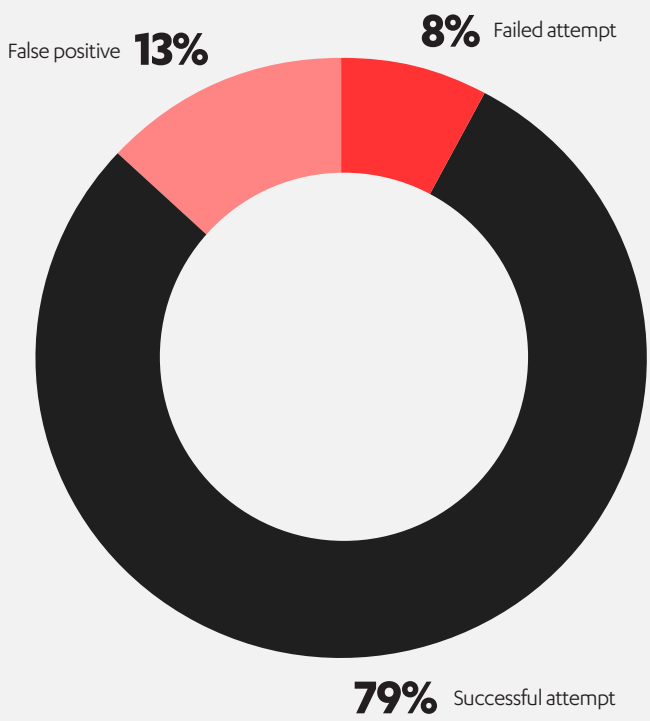


Attacker progress before response

Attacker progress before response

Because incident response investigations are reactive, investigators become involved at different points of the attack, which is reflected in the data. In our experience, incident responders are usually not brought in until a breach has occurred. Cases where they became involved early allowed them to stop the attack while it was progressing. This highlights the value of early detection for organizations, as detecting and stopping attacks sooner rather than later can help limit the damages incurred by victims.

Cases where incident responders became involved in the latter stages of an attack saw the responders focus on investigating the incident and repairing the damage so the victim could get back to business. Damage to the victims varied considerably in these cases. Investigators often found malware left by attackers for various purposes, such as backdoors to ease future access to systems. Fraud, denial-of-service, and data theft were other common malicious acts observed in our investigations.



Investigations by damage to victim

Conclusions

Our investigators often find themselves working with companies that experience actual damage to their business or operations as the result of a breach going undetected. But a surprising number of investigations were conducted due to IT problems or other issues being misunderstood as security incidents by the reporting organization.

Both alternatives create an impression that companies are struggling to detect security incidents: they call incident responders to investigate something "suspicious" rather than knowing whether they're experiencing an actual attack. Organizations can address these issues by developing better detection capabilities, such as by investing in an endpoint detection and response solution or service. Detecting attacks earlier and with greater accuracy will help them respond faster and more efficiently while reducing false alarms.

The observations in this report should be understood as a high level representation of cyber attacks based on investigations conducted in the field. By no means is this exhaustive coverage of all the different methods and resources today's adversaries are capable of using against organizations. It's worth mentioning that targeted attacks – a growing problem – use a greater range of TTPs than their opportunistic counterparts. In spite of this range, the observations in this report largely indicate there are certain patterns that attackers use and re-use consistently. With the right threat intelligence and resources, organizations can better predict and prevent attacks and be better prepared to respond swifty and strongly to any threat.

[1] F-Secure, WannaCry, the Biggest Ransomware Outbreak Ever, https://safeandsavvy.f-secure.com/2017/05/12/wannacry-may-be-the-biggest-cyber-outbreak-since-conficker/

[2] Ellen Nakashima, Russian government hackers penetrated DNC, stole opposition research on Trump, https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html?utm_term=.c555a6f791f1