Secureworks

WHITE PAPER

Why a Glitch Might Be More Than You Think

The Importance of Sweating the Small Stuff

People who have seen the 1999 film The Matrix, with Keanu Reeves, will remember the infamous scene in which the film's protagonist Neo recognizes a glitch in the system before all hell breaks loose.

If you don't remember or you haven't seen the movie, Neo notices a black cat sitting in the stairwell of a simulated reality. Moments later, Neo sees the same cat cross his path a second time. This glitch is quickly mistaken by Neo for harmless déjà vu but luckily his partner Trinity hears what he says and jumps into action to prevent the incoming threat to the team. In the movie, these instances of "déjà vu" are actually someone changing the code in the Matrix, which most likely indicates that a threat is coming. It's a clever way to combine a narrative concept and the software programming, which is central to the film, but it's also very relevant to this paper.

Like Neo in the movie, many security staff face moments that are easy to dismiss as small and insignificant, when in actuality they indicate malicious intent and require action to safeguard systems. Using this concept, we are going to discuss how a small event, or "a glitch", could be more than you think when it comes to cybersecurity. The breaches that can result when one overlooks a minor security event can be broken down into two major phases: **infiltration** and **lateral movement.**

Infiltration (Two Types of Criminals, One Main Attack)

Glitches should always merit suspicion from IT staff. the infiltration phase of a breach. Essentially, there are two types of cybercriminals: the sophisticated cybercriminals who don't want you to know they are in your system, and opportunistic cybercriminals who strike far and wide. Opportunistic cybercriminals are the ones that typically make the headlines; they are responsible for catastrophic attacks like 2017's WannaCry ransomware virus that was detected on 250,000 machines in 116 countries. These threat groups use social engineering techniques, or more directly, an email scam. The Cryptolocker attack was delivered by posing as, for example, Australia Post and luring recipients to click on a link that downloaded malware that encrypted device data. The prevalence of attacks like these highlights how easy it is for threat actors to compromise organisations with phishing attacks.

Attacks like the Cryptolocker Malware are a veritable nuclear strike, not because of the damage they do but because they are overt, unexpected and catastrophic. Everyone is aware of the attack and unfortunately there were a lot of victims. This attack highlighted, for a lot of organisations, that something was missing: user awareness. Organisations started asking "how do we stop people from clicking on links in scam emails?" Many organisations failed to ask the crucial follow-up question; "If people have clicked on this link … What else have they clicked on?" This is critical because sophisticated cybercriminals also use social engineering techniques, like email, to initiate their attacks.

With phishing attacks, there is no big blue error screen once you click on the link. In fact, it is quite the opposite; nothing happens, and the end user deletes the email without raising suspicion. There is evidence that social engineering is the most commonly deployed initial access vector for sophisticated cybercriminals. According to Symantec, phishing rates have increased across most industries and organization sizes, and 76% of businesses reported being a victim of a phishing attack in the last year alone. No company or vertical is immune.

So, to emphasize the point, if end users have clicked on links in the past, opening the door to their organization's data systems, what might they have let in?

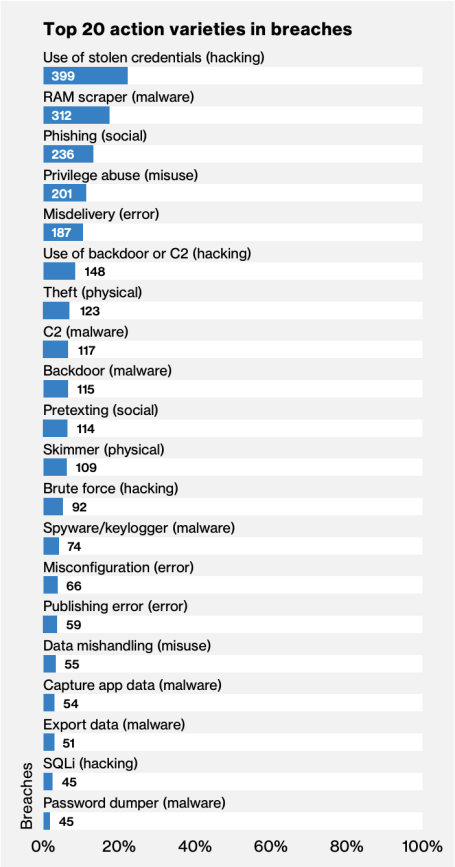

Figure 1: Findings from Verizon's 2018 Data Breach Investigations Report

Lateral Movement (A Glitch Can Be A Clue)

Cybercriminals that have breached your network are going to be looking for things like where your data is kept, what systems you use that they can further exploit, and seeking the golden key: admin credentials.

This exploration of your network by a cybercriminal is known as lateral movement, and it occurs after infiltration. During this lateral movement through a network the intention of sophisticated cybercriminals is to go unnoticed. They do not want to be found so they don't leave many clues, but there are often telltale signs that cannot be ignored. These minor glitches could mean that you have had a breach and need to take action. Some examples of these glitches are:

- Unnecessary outbound traffic to a country in which your organisation does not operate
- Strange network activity from a utilization level: perhaps high compute power from somewhere during low peak times
- Certain files accessed from departments in the organisation that should not really have access, for example a sales person accessing payroll files
- Users with unnecessary privileged access
- Unapproved installed software on devices

If you are seeing these kinds of things happening in your network, then it is time to act. An appropriate analogy here might be when you start hearing a noise coming from your car. Maybe the noise is minor, a rattle coming from somewhere in the engine bay. You have one of two choices: ignore the rattle and continue driving or take the car to a mechanic and have them check the car over for a fault. Most people would have it inspected, aware that if you ignore a rattle coming from the engine bay of your car it is most likely going to get worse, and the worse the noise is generally means the worse the damage is, which in turn leads to a higher cost of repair. The exact same thing is applicable to organisations when it comes to cybersecurity: the worse the breach, the worse the damage, and in turn the higher the cost of repair.

Develop an Actionable Suspicion

The best thing you can do is develop an actionable level of suspicion. This does not mean everyone in IT should be looking over their shoulders in the parking lot or removing their organization's network from the internet. Rather, if you see something unusual, then be analytical rather than dismissive; look into it, ask why it might be happening, and if you believe it to be malicious then engage an expert to dig into the meat, bone and fiber of your network to help you determine if your paranoia is substantiated or not. If you are right, you have just developed the rationality for your board and decision makers to make a call on increased investment in cyber security; if you are wrong, then your board has peace of mind in knowing that their security team is vigilant and, better yet, that nothing has happened. Regardless of the outcome, it is always a success when a security analyst investigates something that doesn't feel right.

Sophisticated cybercriminals don't want to be caught. They want to move through your network without being detected because if they are, they might lose their ability to complete their objective. But remaining invisible is close to impossible, so long as organisations don't ignore the "glitches" that they see in their networks. Have an actionable concern for your systems and investigate glitches by engaging a professional team to provide expertise on what these glitches could mean and whether your suspicion is justified. Doing so might just help to reduce the impact of a cyber breach, but if not, then at least the board of your organisation can rest easy.

Secureworks®

Secureworks® (NASDAQ: SCWX) is a leading global cybersecurity company that protects organizations in the digitally connected world.

We combine visibility from thousands of clients, aggregate and analyze data from any source, anywhere, to prevent security breaches, detect malicious activity in real time, respond rapidly, and predict emerging threats. We offer our clients a cyber-defense that is Collectively Smarter. Exponentially Safer.™

Corporate Headquarters

United States
1 Concourse Pkwy NE #500 Atlanta,
GA 30328
+1 877 838 7947
www.secureworks.com

Europe & Middle East

France
8 avenue du Stade de France 93218
Saint Denis Cedex
+33 1 80 60 20 00
www.secureworks.fr

Germany
Main Airport Center,
Unterschweinstiege 10 60549
Frankfurt am Main Germany
069/9792-0
www.dellsecureworks.de

United Kingdom
One Creechurch Place,
1 Creechurch Ln
London EC3A 5AY
United Kingdom
+44(0)207 892 1000
www.secureworks.co.uk

1 Tanfield
Edinburgh EH3 5DA
United Kingdom
+44(0)131 260 3040
www.secureworks.co.uk

United Arab Emirates
Building 15, Dubai Internet City Dubai,
UAE PO Box 500111 00971 4 420
7000

Asia Pacific

Australia

Building 3, 14 Aquatic Drive Frenchs
Forest, Sydney NSW Australia 2086
1800 737 817
www.secureworks.com.au

Japan
Solid Square East Tower 20F
580 Horikawa-cho, Saiwai-ku
Kawasaki, 212-8589
Japan
81-(44)556-4300
www.secureworks.jp