TRUEFORT

POSITION PAPER

Seizing the Upper Hand

IN RANSOMWARE ATTACKS

+1 201 766 2023 | sales@truefort.com

TRUEFORT.COM

Overview

Over the last several years, ransomware attacks launched by threat actors and cyber criminals have grown more complex and frequent – and often more successful. Headline stories about major ransomware hold-ups have become familiar, almost expected. Then there are the incidents that are never made public. With their backs against the wall, untold numbers of victimized organizations quietly pay exorbitant sums to avert catastrophe.

It's clear that, today, cyber criminals are winning the ransomware war. Their tools and techniques are more powerful and effective than the traditional security measures now being used by enterprises and other organizations.

TrueFort believes it's time to turn the tables in this battle. Companies need to start using faster and smarter cybersecurity defenses in general and more effective ransomware protections, in particular. In short, to keep pace with modern attacks, organizations need to move toward more dynamic, real-time controls that go beyond simply detecting problems. The good news is that these advanced, defensive weapons already exist. It's time for enterprises to use them to regain the upper hand in the war against cyber criminals and their ransomware attacks. This paper details how organizations can start fighting back.

> To keep pace with modern attacks, organizations need to move toward more dynamic, real-time controls that go beyond simply detecting problems.

Background –

How Enterprises Got Outpaced and Outmaneuvered

Today, most security controls are static.
They were hand-coded, and then thoroughly tested before being deployed into production. It's a process that typically takes weeks or even months, and results in a resource that is difficult and time-consuming to change in any significant way.

Meanwhile, in the attackers' camp, things are looser and much more fast-paced. Threat actors develop highly sophisticated command and control environments that enable them to monitor and adjust their malware on a near-real-time basis, always staying a step ahead of traditional defenses.

This gap between the slower and more careful enterprise approach, and the much faster and more responsive 'run-and-gun' tactics of the attackers is a primary contributing factor in the enormous increase in ransomware attacks over the past few years.

Let's look at some notable examples of how threat actors have used their greater speed and dexterity to drive successful ransomware take-downs.

In 2017, there were multiple ransomware attacks, including NotPetya, which at the time, became the costliest cyberattack in history. For its time, NotPetya was shockingly sophisticated. It was written in a way that enabled it to propagate automatically and very rapidly. So fast, in fact, that it was able to take down more than 15,000 servers at a major pharmaceutical company in less than 90 seconds. While unprecedented at the time, the speed and automation that was built-in to NotPetya is now commonplace with many of the ransomware toolkits now available on the dark web.

More recently, the Colonial Pipeline ransomware attack earned headline news coverage worldwide. In that sophisticated attack, cyber criminals were able to steal over 100GB of data in under two hours. Indeed, Colonial wasn't even aware of the attack until they received the ransom demands from the Eastern European crime ring responsible for it. Again, the advanced nature of the attackers' tooling and techniques enabled the perpetrators to move faster than the victimized organization.

Speed, however, is only one aspect to consider. Another major factor that cyber criminals have leveraged to their advantage is the sophistication of their attacks, which has increased markedly. Threat actors are writing custom code, specifically designed to detect security controls such as endpoint detection and response (EDR) tools. Where EDR protections are detected, the attack package then either automatically works around the control or remains dormant to avoid detection.

The group behind the Solar Winds attack this year provides an example of this functionality. With that attack, the code was written to avoid targets using specific types of EDR tools since the cyber criminals knew that those specific tools were capable of detecting their malware.

In all cases, the data point to the same conclusion. Hand-crafted, heavily tested and static security controls are simply incapable of protecting against these types of attacks. To change the negative direction this war has largely taken over the past few years, and to stop the woeful outcomes, a more viable strategy is required.

SUCCESSFUL RANSOMWARE TAKE-DOWNS

2017

NOTPETYA

Cyber Criminals took down more than **15,000 servers in less than 90 seconds.**

2020

COLONIAL PIPELINE

Cyber criminals were able to steal o**ver 100GB of data in under two hours**.

2021

SOLAR WINDS

Cyber criminals used code that was written to avoid targets using specific types of EDR tools.

Faster Detection —

A Good Start but Not Enough

Frustrated with poor results, some companies have decided to take action. They have started to adopt more advanced technologies in their threat defenses, such as machine learning and artificial intelligence. However, in most of those cases, the technology is being deployed in va detect-only manner. That means they are only capable of generating alerts about potential problems. Thus, instead of initiating rapid responses, they merely hand off what they've found to a SOC for triage and response. As was made painfully clear by NotPetya, being able to detect a problem automatically is insufficient if the response time is hours or days.

It is reasonable to assume the sophistication of threat actors will only increase. As long as cybercrime and ransomware remain profitable for criminal organizations, they will continue to invest in new and innovative techniques for compromising and bypassing security controls. And where they are willing to invest to create fully automated attack toolkits, cybersecurity professionals are going to need to respond with more automation in their detection and response capabilities. This means moving away from hand-crafted, static security controls and instead, implementing automated, intelligent, and preventative controls that provide more autonomous, and even more accurate, response capabilities to the computer.

> A more effective response means moving away from hand-crafted, static security controls and toward automated, intelligent, and preventative controls that provide more autonomous, and even more accurate, response capabilities.

More Speed and Dexterity Through Automation

What, exactly, do "automated, preventative controls" look like?
How are they different from traditional security controls?
Most importantly, how can they lower the risks and lessen the impacts of ransomware?

HERE ARE THREE, ILLUSTRATIVE EXAMPLES:

1 Preventing Mass Logins

Most organizations have a relatively small number of system accounts that have legitimate reasons to log into large numbers of devices in a short period of time. Backup services, for example, will often log into dozens or hundreds of servers every night. Patching systems may log into thousands of end points per hour. However, those accounts should be both well-known and tightly controlled. An organization could, therefore, develop a security control that monitored for mass login events from a single account and automatically disable that ID when it hits a predefined threshold. Using the NotPetya example, imagine if the pharmaceutical company only lost a few dozen servers before their automated controls kicked in and disabled the compromised account. It would have saved significant time, money and effort spent on recovery. In the case of ransomware, it can help in a similar fashion.

2 Model-driven Data Loss Prevention

Historically, Data Loss Prevention or DLP, has been only moderately successful due to this technology's tendency to generate high numbers of false positives, and as a result, 'noisy' environments. And due to their real or perceived negative impacts on business operations, the false positive issue has also made organizations less willing to deploy DLP in full blocking mode. However, through advancements in machine learning, organizations can now establish baseline patterns of behavior for data transfer scenarios. Then, when anomalous activity is detected, controls can automatically block data from leaving the environment on a per-user basis. Machine learning greatly reduces the number of false positives and being able to apply the control on a per-user basis greatly reduces the impact of what few false positives may remain.

3 Anomalous Process Termination

The concept of process whitelisting has been around for quite some time, but this technique has been generally avoided due to its management complexity. And like DLP, it has a reputation for high false positive rates. Here again, however, with recent advances in machine learning, organizations can now develop models to help provide baseline patterns of "normal" behavior for their high-risk servers. Once a baseline has been established, controls can be implemented to automatically terminate processes that fall too far outside of the established normal patterns.

Bundled together, these three example controls could help an organization to better protect itself against ransomware, both from initial infections and subsequent impacts.

Steps on the Path to Success

Some people argue that automated, preventative controls, such as described above, bring significant risk of operational disruption. While there may be some truth to this, there are examples – such as the high frequency trading (HFT) sector of the financial services industry, that provides proof that computers can operate fully autonomously in high-risk environments.

As critics will point out, the history of HFT was not without problems. Indeed, in 2010, there was the famous "Flash Crash" caused primarily by HFT. However, HFT did get sorted out fairly quickly, and some of the lessons learned in that experience can be applied toward making the path towards automated security controls smoother, including:

- **Algorithmic boundary controls.** Any automated control should have upper and lower thresholds assigned to it, as appropriate, to prevent runaway events. As an example, a boundary control might be defined to prevent more than three system accounts from being automatically disabled in a single, 30-minute period.
- **Adopting Immutable Infrastructure.** Borrowing a page from the cloud computing book, migrating to immutable infrastructure also delivers benefits when creating automated, preventative controls. Immutable infrastructure operates more predictably, making the models supporting these preventative controls more accurate as well.
- **Leverage red teaming concepts for testing.** Any environment that relies on automated controls needs to have a separate, robust test environment in which red teams and sysadmins alike can experiment with all kinds of "what if" scenarios, and try to break things. Being able to refine and tune models in a non-production environment greatly reduces the risk of bad things happening in production.

These techniques, combined with an agile, DevOps-based approach, enable security organizations to not only develop controls that can detect ransomware and other sophisticated cyber attacks rapidly, but also respond to them automatically in real time.

Conclusion

It's time to close the gaps and eliminate the speed and dexterity advantages that cyber criminals have used to cause chaos and get rich from ransomware and other sophisticated exploits. It's time for enterprises and other organizations to seize the upper hand. With intelligent, rapid detection coupled with automated, real-time response capabilities, companies can start winning battles on their way to winning this war.

At TrueFort, we firmly believe that these kinds of dynamic defenses are the only way organizations will be able to mount and maintain effective defenses against the increasingly sophisticated attacks that are happening today, and that will surely continue into the future.

Intelligent automation is the key, and effective solutions are already available. There are only two prerequisites: recognizing the dire nature of the problem, and having the determination to change the status quo. In our view, the path forward is clear.

REQUEST A DEMO

& See What You've Been Missing

ABOUT TRUEFORT

TrueFort reduces business risk for security-focused enterprises striving for zero or lean trust application environments. Our innovative and uniquely application-centric Fortress platform delivers comprehensive realtime cloud-to-the-ground insight, protection and automated response with patented machine intelligence and a single or bring-your-own agent. Fortress overcomes the application security blindspots inherent in legacy infrastructure-centric tools, providing unparalleled visibility and protection for applications in on-prem, hybrid and cloud environments and for security teams across the enterprise. Fortress speeds response times, minimizes the blast radius of compromises, prioritizes resources, and enhances application risk posture.

TRUEFORT

3 West 18th Street
Weehawken, NJ, 07086
United States of America

+1 201 766 2023
sales@truefort.com

TRUEFORT.COM