Research Report

First Quarterly
2022 Review

CYBER THEORY

CYBER THEORY

We are a full-service cybersecurity marketing advisory firm. We constantly collect and analyze the latest customer data segmented by security practitioner, industry and region. Our extensive knowledge model allows us personalized targeting of each and every cybersecurity buyer persona. With strategic insights from global education services, media providers, intelligence analysts, journalists and executive leaders, we're always adapting to the latest industry trends. Our network of relationships encompass all aspects of cybersecurity as well as the related fields of fraud, audit, compliance and risk management.

CONTACT INFORMATION

cybertheory.io

212.518.1579 • info@cybertheory.io

530 7th Avenue, New York, NY 10018

Table of Contents

The Beginnings of 2022 are off to a Predictable Start

Our first quarter data suggests a continuation of the most profitable and workable cyberattack schemes from the prior four quarters with some newly active approaches and mini-markets (for now) to keep the pressure on our defenses.

Crypto Markets

We have seen crypto hacking surge this first quarter as compared to prior years, with 77 cases reported, representing over $1.2 billion lost to criminal actors. The Ethereum blockchain led the way with 18 hacks worth over $635 million.

As is often the case, the rapidly popular currency has ignored best development practices resulting in exposure to and exploitation of revealed vulnerabilities in both blockchain implementations and flaws in the code base.

Speed Kills

The crypto market has reached a capitalization of $2.27 trillion on the back of a bull rally across the industry.
It will be an active year in the crypto markets, and while most folks mistakenly think the market is under-regulated, it is the most regulated market in Financial Services, so theoretically, one is safer in a FinTech blockchain with cryptocurrency than in a traditional database with fiat. As indicated, the best preventions are always the best cures, so slow down, apply fixes to known bugs, understand your GitHub content, find and dismember vulnerabilities before you start and QA your code base to death.

Ransomware

Ransomware continued and will continue to dominate the 2022 threat landscape, as we witness operators taking new approaches with new techniques.

A significant ransomware trend in 2021 was the increase in adversaries expanding their threats beyond data encryption. Multiple ransomware groups pivoted to stealing and exfiltrating data before encrypting it, then demanding payment to prevent the data from leaking publicly on a dark web site. While this practice isn't new (it dates back to at least 2019), what was significant in 2021 was the number of groups who adopted this approach—to the point where it became the standard.

Adversaries realized they could demand payment for more than just the threat of a data leak or encryption. An adversary known as Fancy Lazarus (no affiliation with Fancy Bear or Lazarus Group) extorted victims by threatening to conduct a distributed denial of service (DDoS) intrusion if they didn't pay.

There is no one simple way to prevent ransomware, and at the end of the day, everything involving malware as an attack vector is ransomware and should be viewed in that context.

It's critical to regularly update software, as we often see ransomware pop up after operators exploit a vulnerability in an internet-facing application. Additionally, internet-facing remote desktop protocol (RDP) connections without multi-factor authentication (MFA) are a common ransomware vector, making MFA for any accounts that can log in via RDP a high priority.

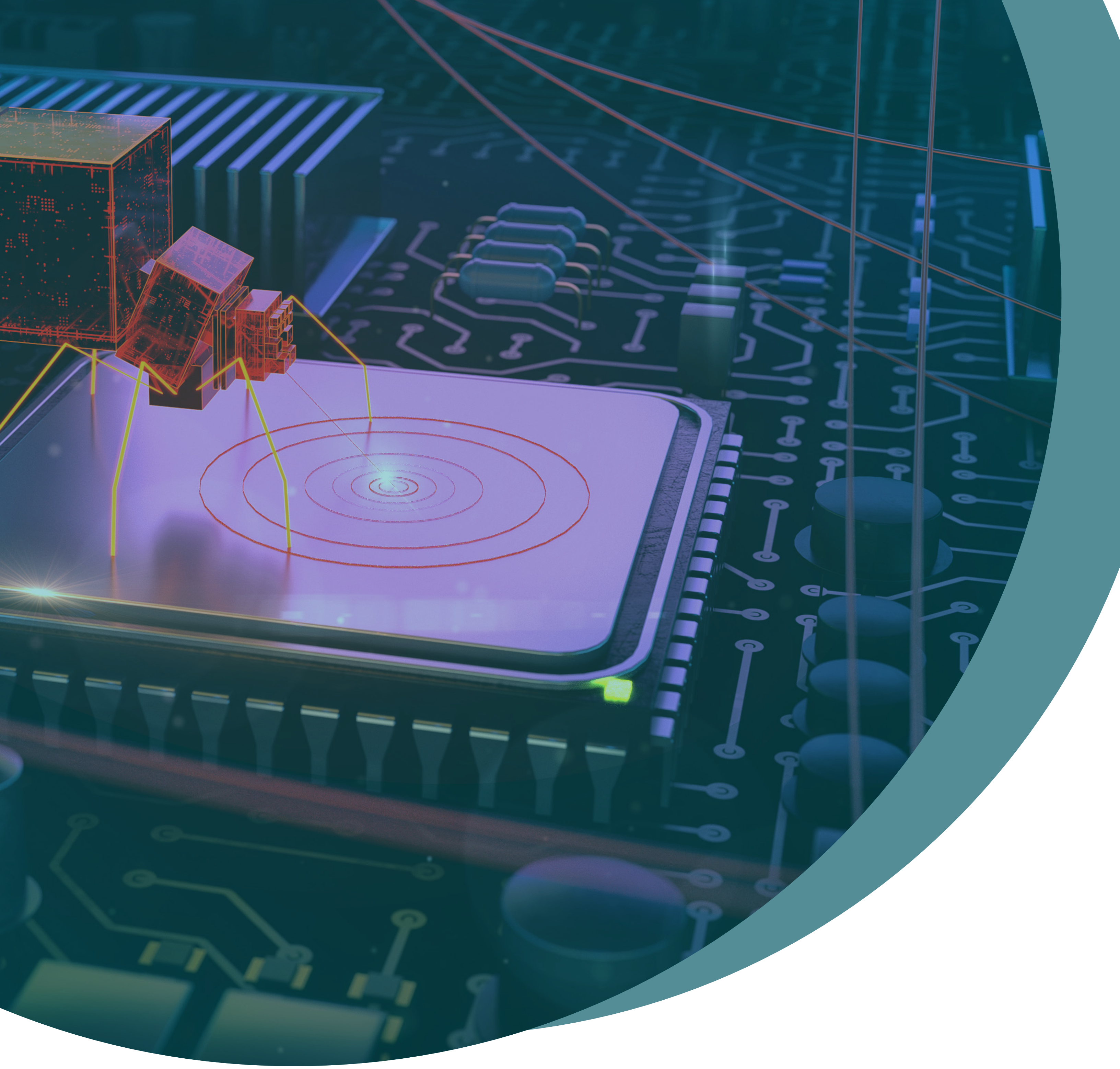
MFA is not convenient to implement, but end-users and customers must come to grips with the reality that an early line of defense is identity proofing and a big part of that is authentication. Without it, we retain large holes through which bad guys easily navigate.

It's also important to remember that backups are no longer sufficient ransomware protection. While creating

offline backups is an excellent security practice and may help restore an environment after a ransomware intrusion, organizations cannot rely on backups entirely because adversaries regularly exfiltrate data before encryption, rendering backups useless although this activity also offers potential opportunities for detection. We can only detect what we monitor however and it appears that state of that maintenance has not gained much traction in the last year – we still do not monitor our operations sufficiently.

Since you don't know what you can't see, it baffles us as to how one would expect to be able to detect and deter with robust monitoring, yet we see few signs of it even now.

Backups will allow an organization to get back up and running more easily, but will not protect you against leaked data.
We will see more ransomware because it works.



> ...tools will help you detect malicious post-exploitation activity in the event an adversary gains access to your network through a trusted third party.

Supply Chain Compromise

Starting with SolarWinds, Kaseya and NPM package compromises mid-year, and ending with Log4j, supply chain compromises were a major disruptive trend in 2021. These incidents continued into Q1 2022 and will pervade throughout the year.

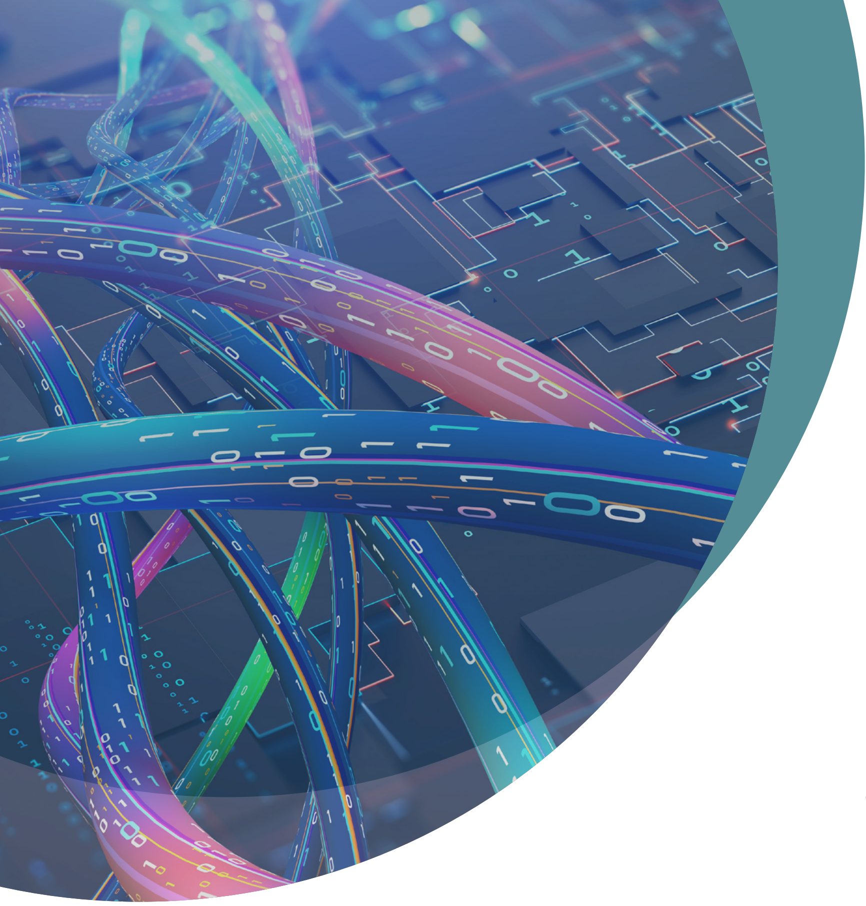
A supply chain compromise occurs when an adversary compromises a software developer, hardware manufacturer or service provider and uses that access to target customers who use the affected software, hardware or service.

For example, the SolarWinds and Kaseya incidents involved an adversary compromising update servers to target customers of the companies' IT management software. Separately, NPM package and Log4j incidents involved adversaries exploiting open source libraries in sweeping compromises that impacted products that use Log4j or NPM packages as a dependency – as well as anyone who uses those products directly.

Because Supply Chain compromise is so destructive and self-directed, it will continue as a major threat through 2022.

Unfortunately defending against it requires no magic beans – an accurate inventorying of all the hardware, software and service providers you rely on and trust is key. While it sounds too old-school, normal old-school defense-in-depth strategies can also help prevent supply chain compromises from turning into impactful intrusions.

Endpoint detection and response (EDR) tools coupled with network detection **tools will help you detect malicious post-exploitation activity in the event an adversary gains access to your network through a trusted third party.** While there may be nothing you can do to prevent a dependency or a vendor from being compromised, there is quite a lot you can do to detect and prevent follow-on compromise, and you should.



Vulnerabilities

Breaches do not occur without cooperation from the supply side.

In 2021, we have had several climb to prominence. ProxyLogon and ProxyShell targeted Microsoft Exchange servers and affected a massive number of systems, sometimes leading to ransomware deployment. The exploitation of vulnerabilities in Kaseya's VSA appliance software also led to ransomware deployment on some of the thousands of organizations that used Kaseya software for remote administration of endpoints.

In the latter half of the year, adversaries exploited multiple vulnerabilities in Zoho's ManageEngine suite of products. PrintNightmare and an MSHTML vulnerability caused a ruckus among the security community and media; however, their actual impact appears to have been limited. Cybersecurity, as we are learning, is not a passive sport.

There are defensive measures and protective measures, but there are also responsibilities we must embrace that keep our environments clean and stable. We all know now that vulnerabilities are just flaws in code – an actual threat must exploit that vulnerability.

Given the frequency with which vulnerabilities are disclosed and the ease with which adversaries can exploit newly reported weaknesses, particularly in common applications, there are lots of research teams working on the problem 24/7 like Red Canary, which focuses on identifying and detecting the behavior we observe surrounding exploitation of a vulnerability.

We recommend all organizations leverage the same resources. Understanding the threats and the ways in which adversaries operate in compromised networks allows defenders to improve and protect against malicious activity regardless of the means by which their environment is accessed. We have seen steadily increased growth in Q1 and expect it to continue throughout the year.

Expanding Threats

We see tons of threats expanding daily here, so it is of little help to identify each SocGholish that shows up. Suffice it to say that there are many and that Q1 showed no signs at all of slowing down or taking a turn – when something works, you don't fix it.

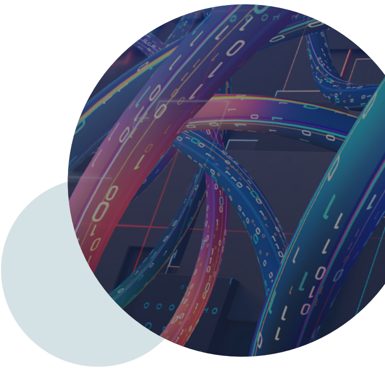
It is far more important to realize that we actually have far greater tools and resources, practices and techniques that we can leverage in our best defense than we thought. A focus on published vulnerabilities, disciplined patching, defensive tools and processes to combat ransomware and supply chain attacks will go a long way to raise our shields against the continuing trends of 2022. But we also need a new, overall strategic model for cybersecurity, or we will be doomed to continue fighting a losing war.

A New Strategic Model

Which is good for no one, other than the bad guys.

We need to step back, take a systems thinking view, contextualize our approach against a larger context than just the frameworks we have embraced and ask ourselves is there another way to expand these elements into a different form of relationship that may work better?

In our view, re-examining your cybersecurity strategy through the lens of the Zero Trust foundation principles and then identifying those pieces that need to be pulled into alignment with those principles is a great place to start.



CYBER THEORY

cybertheory.io
212.518.1579 • info@cybertheory.io
530 7th Avenue, New York, NY 10018