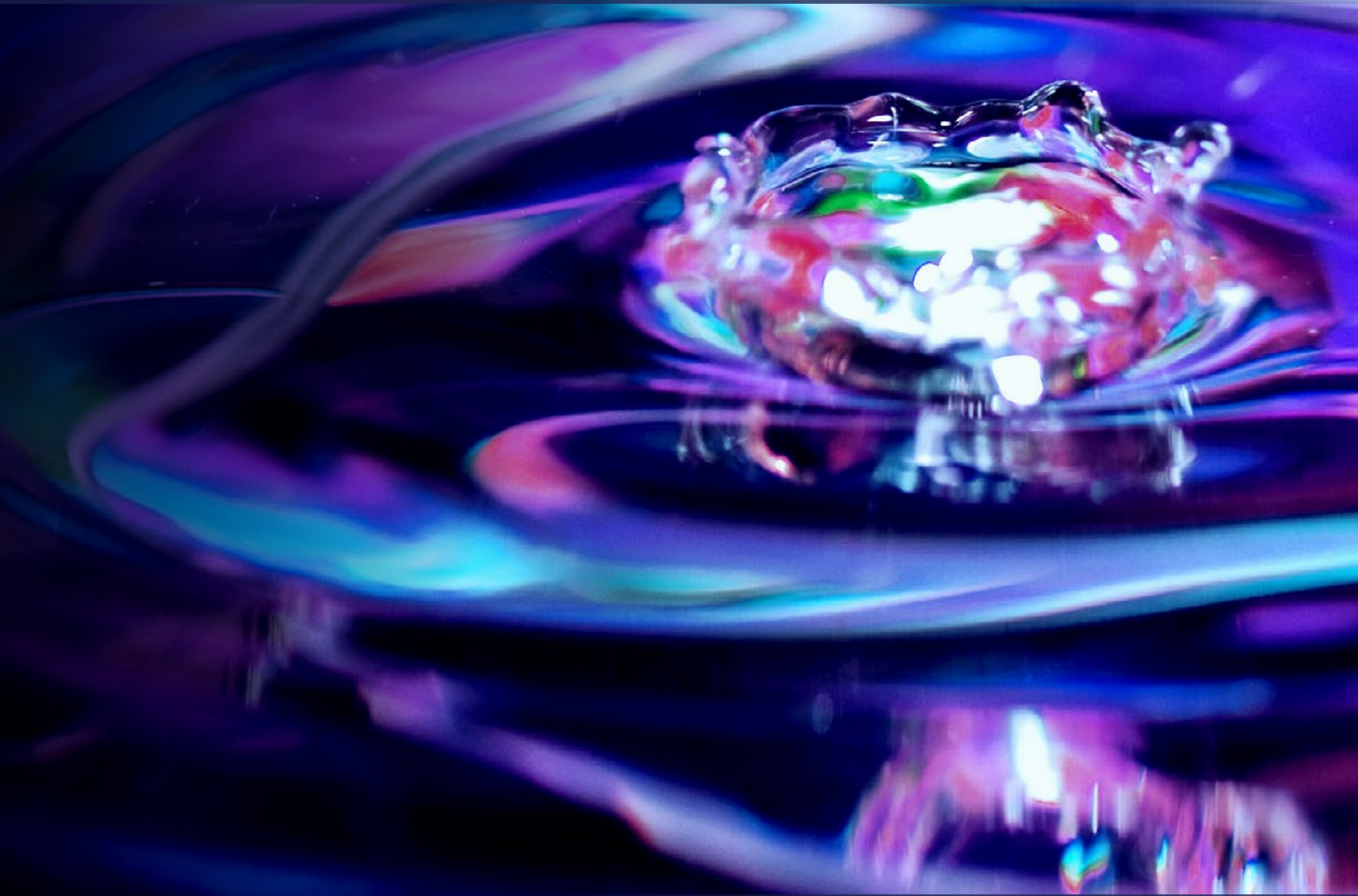
3RD **RIPPLES** EDITION

RIPPLES ACROSS THE ATT&CK SURFACE

ANALYZING **TOP ATT&CK TECHNIQUES** USED IN MULTI-PARTY CYBER EVENTS



A collaborative research project between

riskrecon by | Cyentia INSTITUTE

TABLE OF CONTENTS

Sometimes, seemingly small, isolated events can trigger widespread consequences. Such is the case when the effects of one organization's security incident spill over to impact third parties and the broader supply chain. We refer to these spillover effects from multi-party incidents as "ripple events," and they've been a focus of our research for several years now.

Our latest study analyzes nearly 900 historical ripple events to identify the top MITRE ATT&CK techniques used. We seek to understand how these ripples occur and propagate, so your organization doesn't get swept up in their wake.

KEY TAKEAWAYS

7X MORE

MULTI-PARTY SECURITY INCIDENTS TYPICALLY COST SEVEN TIMES MORE THAN SINGLE-PARTY EVENTS.

EXPLOITING PUBLIC-FACING APPLICATIONS RESULTS IN THE LARGEST PROPORTION OF FINANCIAL LOSSES FROM MULTI-PARTY SECURITY INCIDENTS.

SYSTEM INTRUSIONS ARE THE RISKIEST TYPE OF RIPPLE EVENTS, SURPASSING ALL OTHERS IN FREQUENCY, TOTAL FINANCIAL LOSSES, AND THE NUMBER OF THIRD PARTIES IMPACTED.

RIPPLE EVENTS RESULTING FROM INSIDER MISTAKES ARE TWICE AS COMMON AND 800 TIMES COSTLIER THAN THOSE INVOLVING INSIDER MALICE.

TARGETING VALID USER ACCOUNTS AND EXPLOITING TRUSTED THIRD-PARTY RELATIONSHIPS ARE THE MOST COMMON INITIAL ACCESS TECHNIQUES LEADING TO RIPPLE EVENTS.

MALICIOUS CODE INJECTION AND OBFUSCATION WERE ASSOCIATED WITH 100% OF REPORTED FINANCIAL LOSSES AND 87% OF THIRD PARTIES IMPACTED BY MULTI-PARTY SECURITY INCIDENTS.

METHODOLOGY

About the data used in this report

This study leverages Zywave Cyber Loss Data, containing over 130,000 cyber events collected from publicly verifiable sources.

THREE FEATURES MAKE THIS DATASET UNIQUELY SUITABLE FOR THIS RESEARCH:

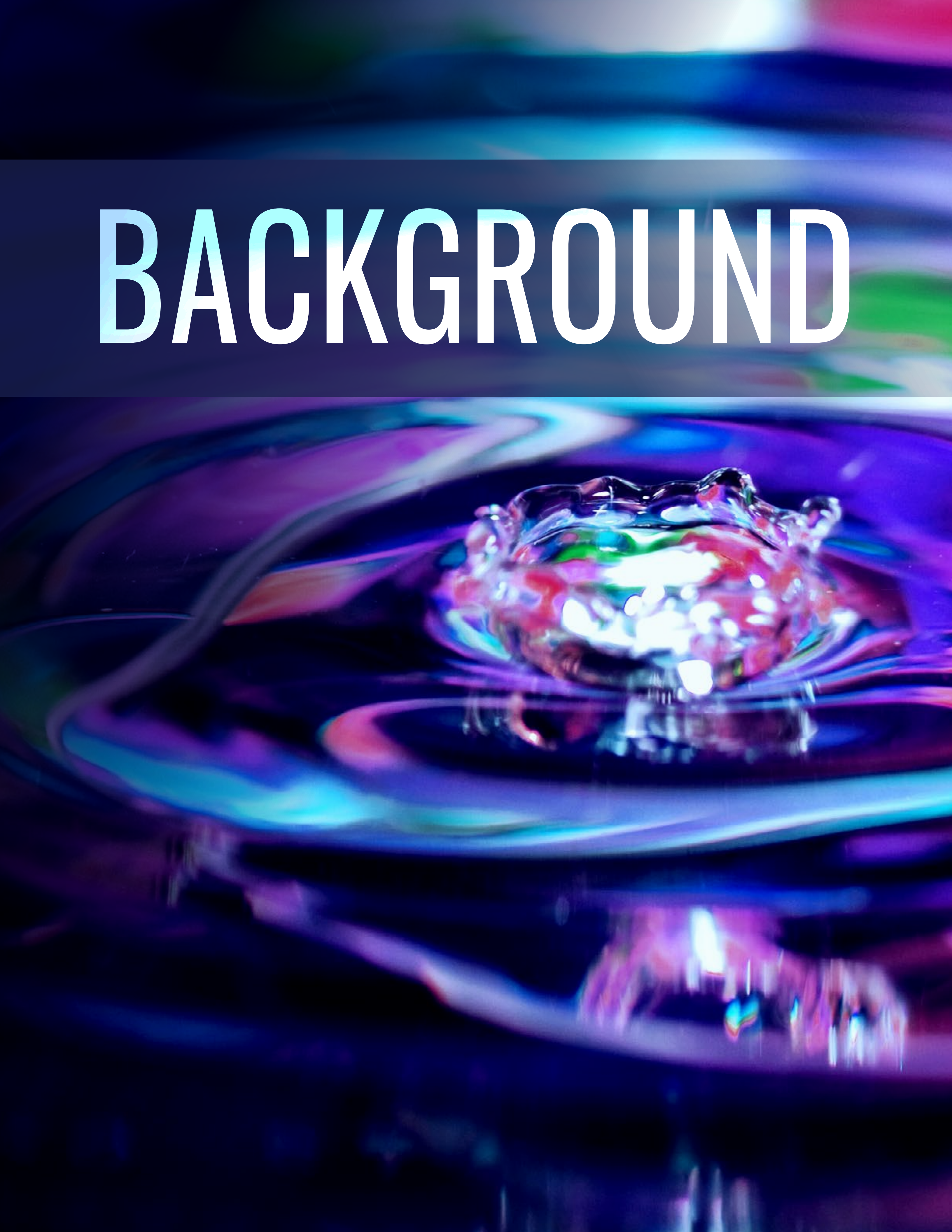
1. It has comprehensive coverage across a wide array of incidents
2. It links organizations involved in or impacted by a common incident
3. It tracks losses publicly disclosed in the wake of those events.

From this, we identified 830 incidents that rippled outward, impacting an additional 5,820 downstream organizations. These multi-party events form the corpus of our current analysis.

DISCLAIMER: Classifying Incident Patterns and ATT&CK Techniques

The Cyentia Institute conducts additional processing of Advisen's cyber loss data to enrich it with information, including incident patterns and ATT&CK techniques. We do this using a combination of methods. Where possible, we use standard fields in the Zywave dataset to assign patterns and map them to their equivalents in ATT&CK. Beyond that, we use natural language processing on incident descriptions and malware behavioral analysis to support classification. Larger or high-profile loss events often trigger manual assignment of techniques by one of our analysts. In short, we do whatever we can to reasonably infer incident types and the techniques involved.

BACKGROUND



WHAT'S A RIPPLE EVENT?

A QUICK EXAMPLE...

In May 2020, Blackbaud was hit by a ransomware attack. As a software firm that sells administrative tools to non-profits and educational institutions, Blackbaud was able to prevent attackers from blocking system access; however, the attackers still managed to successfully exfiltrate sensitive data, including banking information and social security numbers.

The impact of this data breach quickly spread far beyond Blackbaud, affecting hundreds of companies with business ties to the software vendor. These victims downstream (those organizations affected by the breach beyond Blackbaud itself) of the breach spanned eight industries, including education, healthcare, administration and logistics, hospitality, and more. Publicly reported losses across all of the victim organizations exceeded $47M.

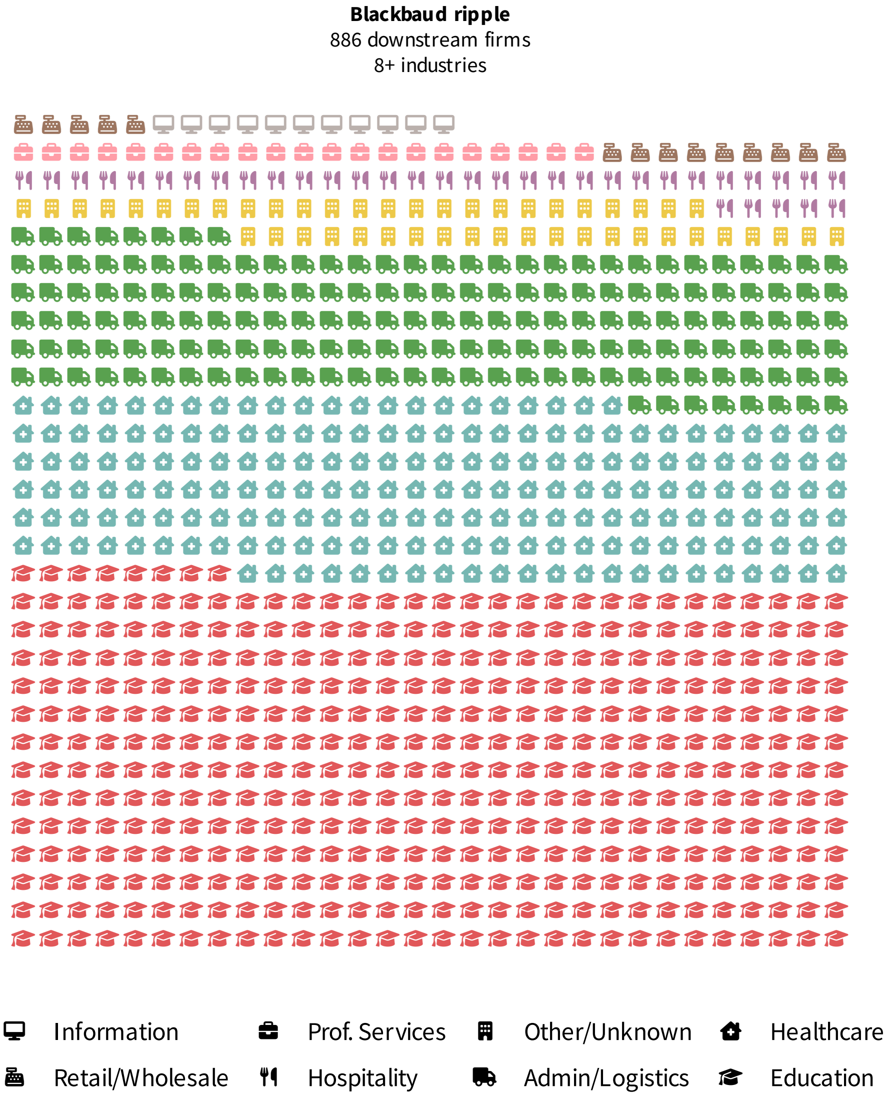


FIGURE 1: INDUSTRIES OF FIRMS IMPACTED BY THE "RIPPLES" GENERATED FROM BLACKBAUD INCIDENT IN 2020

19% of Victims in Admin/ Logistics

22% of Victims in Healthcare

45% of Victims in Education

The ransomware attack on Blackbaud represents one of many multi-party security incidents that have hit the scene in recent years. We call these "ripple events" because they originate from a central victim and then spread outward, impacting various third parties. These ripple events are particularly concerning as they can trigger losses without any security failures by the downstream parties (as was the case with the Blackbaud incident).

In 2019 we introduced the concept of ripple attacks with "Ripples Across the Risk Surface," which analyzed more than 800 ripple events in order to understand broad trends around frequency and impact. Two years later, we updated and extended that analysis with a second installment of "Ripples." Next, we conducted an in-depth examination of threat methods and vectors associated with the 50 largest ripple events in the "Tsunami edition" of the Information Risk Insights Study (IRIS) series.

The current study is an effort to combine the high-level analysis of numerous incidents from "Ripples" with a low-level investigation into a subset of events in "Tsunami." However, before diving into that analysis, it's fitting to review some key lessons from our prior research on ripple events.

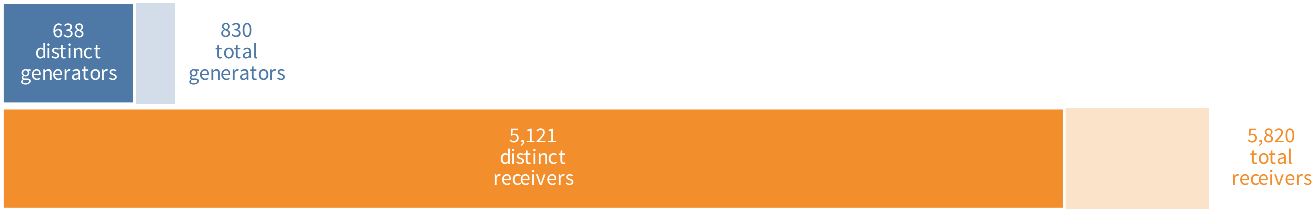
LESSON 1: Ripple events are increasingly common

Ripple events have become more common as businesses continue to modernize and weave complex digital interdependencies with each other. Based on our previous analyses, multi-party incidents have increased at an average rate of 20% per year over the last decade.

LESSON 2: Ripple events can spread far and wide

Ripple events are particularly concerning because their impact can spread far beyond the initial victim. As mentioned, we previously studied over 800 ripple events. What we didn't mention is that these events generated downstream effects that impacted nearly 6,000 other organizations. That means ripple receivers outnumber generators at a 7-to-1 ratio. Furthermore, some ripple events swell significantly larger, affecting hundreds of third and fourth parties (refer, once more, to the Blackbaud example).

FIGURE 2: NUMBER OF CENTRAL VS. DOWNSTREAM ORGANIZATIONS AFFECTED BY RIPPLE EVENTS



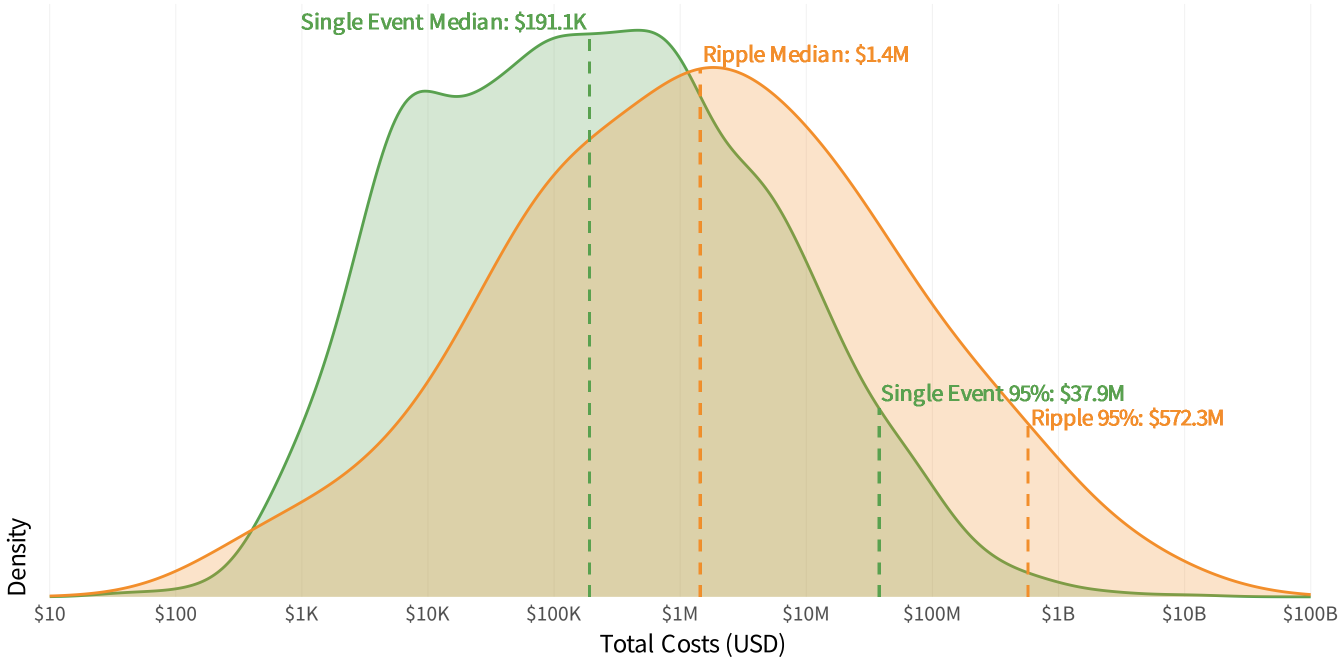
We examined more than 800 ripple events, revealing that these events, in turn, had repercussions on nearly 6,000 other organizations, highlighting a notable 7-to-1 ratio of ripple receivers to generators, with certain ripple events considerably amplifying their impact on hundreds of third and fourth parties.

LESSON 3: Ripple events cause higher financial impact

Ripple events are also more costly than single-party incidents. As the chart below indicates, the median loss for multi-party events is $1.4M, compared to $191K for a single-party incident. Even more concerning, the distribution's extreme "tail" is much fatter for ripple events. The loss magnitude at the 95th percentile ($572M) is 15 times higher than that of single-party events.

This provides compelling incentive for organizations to be aware of the risks associated with multi-party incidents and understand how to manage them. And that's exactly what we hope to accomplish in this report by investigating common threat patterns and techniques that generate ripple events.

FIGURE 3: DISTRIBUTION OF TOTAL LOSSES FOR SINGLE-PARTY INCIDENTS VS. RIPPLE EVENTS



ARE RIPPLE EVENTS DIFFERENT FROM SUPPLY CHAIN ATTACKS?

Yes. All supply chain attacks are indeed ripple events; but, not all ripple events are supply chain attacks. Compromising hardware or software components is not necessary for generating downstream loss events.

For example, if a data aggregator is breached, the owners/providers of that data may suffer losses even if their systems remain uncompromised.

EXPLANATION OF TERMINOLOGY

We categorize all incidents according to common patterns of threat actors, techniques, vectors, and technical impacts, as defined in the list below. These patterns are intended to represent the high-level scenarios we often encounter on risk registers for assessment and reporting purposes.

ACCIDENTAL DISCLOSURE: Data stores that are inadvertently left accessible to unauthorized parties, usually due to misconfigurations by the data custodian.

DOS ATTACK: Any attack intended to render online systems, applications, or networks unavailable, typically by consuming processing or bandwidth resources.

INSIDER MISUSE: Inappropriate use of privileged access, either by an organization's employees and contractors or by a trusted third party.

PHYSICAL THREATS: Threats that occur via a physical vector, such as device tampering, snooping, theft, loss, sabotage, and assault.

PRIVACY: Events that violate various privacy laws and regulations and don't fall into one of the other patterns (e.g., a breach that triggers GDPR fines would still fall under System Intrusion).

RANSOMWARE: A broad family of malware that seeks to encrypt data with the promise to unlock it upon payment or seeks to completely eradicate data/systems without the pretense of collecting payment.

SCAM OR FRAUD: Any incident that primarily employs various forms of deception to defraud victims of money, property, identity, information, and so forth.

SYSTEM FAILURE: All unintentional service disruptions resulting from system, application, or network malfunctions or environmental hazards.

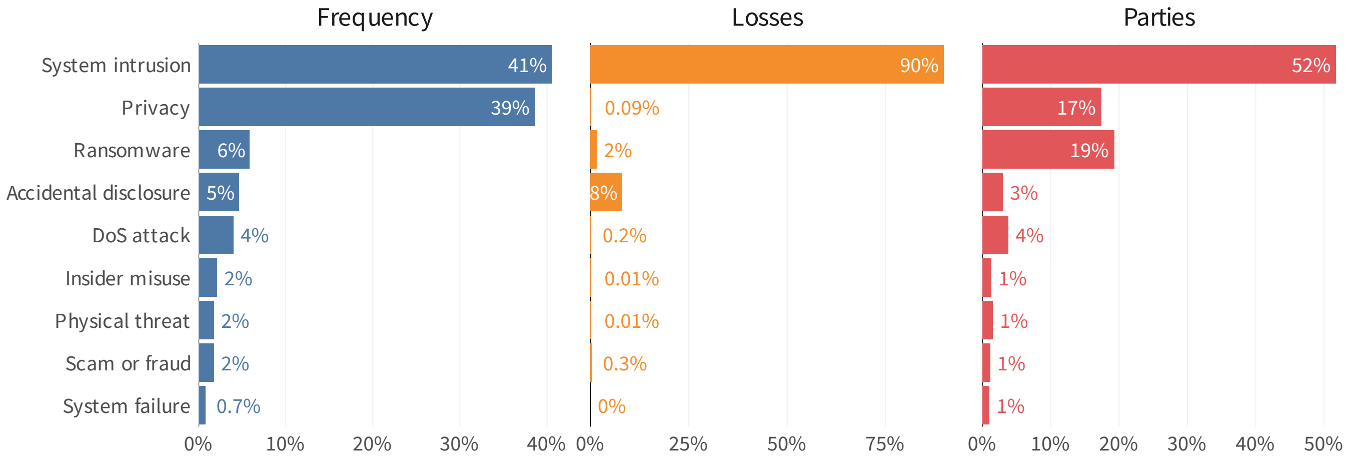
SYSTEM INTRUSION: All attempts to compromise systems, applications, or networks by subverting logical access controls, elevating privileges, deploying malware, and so on.

WHERE NEW RESEARCH BEGINS

In this section we are examining how the incident categories in this research compare across three statistics that make the most impact in ripple events.

In the chart below, it is clear the system intrusion is the clear leader for frequency, losses, and downstream parties affected. This pattern is particularly dominant for losses, where it's associated with nine out of every 10 dollars lost from ripple events. The lesson? Once attackers are inside your (or your partners') network, they can cause extensive damage. Third-party risk assessments focusing on access controls and cyber hygiene would seem well-justified—a theme we will revisit when analyzing ATT&CK techniques.

FIGURE 4: COMPARISON OF KEY STATS ASSOCIATED WITH BROAD CATEGORIES OF RIPPLE EVENTS



Privacy-related incidents feature prominently in ripple events, ranking second by frequency and third by the number of third parties affected. This serves as a reminder that "ripples" come in many forms, including fines and penalties for violating privacy laws that extend beyond the original victim firm.

Considering the infamy of ransomware, it seems odd to see this pattern sitting at a very distant second on the frequency chart, accounting for just 6% of all events. It is perhaps even more surprising that ransomware accounts for such a tiny fraction of financial losses. We suspect this is due to the non-payment and underreporting of ransoms. It's also partly because the research timeframe stretches back to a period when ransomware was not as prevalent as it is today. The frequency and losses would represent a higher percentage if we recreated this chart for the past three years—but it still would not approach the level of system intrusions.

The relatively low frequency and impact of insider misuse will likely raise some eyebrows; however, this aligns with the findings of other notable studies (e.g., Verizon's "Data Breach Investigations Report"). It is worth noting that non-malicious insider activity, in the form of accidental disclosures, is twice as common and 800 times more costly than the malicious variety. Insider malice generates more headlines; but insider mistakes cause more significant harm.

2023 NEW FINDINGS

OBSERVED ATT&CK TECHNIQUES

Broad categories are instrumental for understanding the circumstances that lead to ripple events. However, additional details about the tactics, techniques, and procedures (TTPs) used by threat actors is necessary for effectively mitigating these incidents.

In the following section, we use MITRE ATT&CK to dive deeper into ripple event mechanics. ATT&CK is rapidly becoming the common language for adversary tactics and techniques used across the cybersecurity industry. A major benefit of ATT&CK is that it enables readers to easily find definitions and examples of each referenced technique and to explore a wealth of information on associated threat groups, malware, mitigations, attack simulations, etc.

Unfortunately, public disclosures or media coverage of security incidents rarely provide a detailed list of the involved ATT&CK techniques. Evidence collected via a digital forensics investigation is generally needed for that purpose. However, using a combination of analytical techniques, we validated the ATT&CK techniques for 23% of the primary incidents in our dataset.

While this percentage might not seem like much, keep in mind that a good chunk of these events fall outside the scope of ATT&CK by their nature (e.g., insider, physical, and privacy-related events). Furthermore, those incidents for which we were able to identify ATT&CK TTPs represent a higher proportion of recorded financial losses (35%) and impacted third parties (48% of the total number of affected companies). This suggests that we do, at least, cover a majority of the more important incidents.

We've organized identified techniques into three key stages of an incident: initial access, post-compromise (execution through lateral movement), and exfiltration and impact. In this section, we present the most frequently observed and impactful techniques for each of these stages.

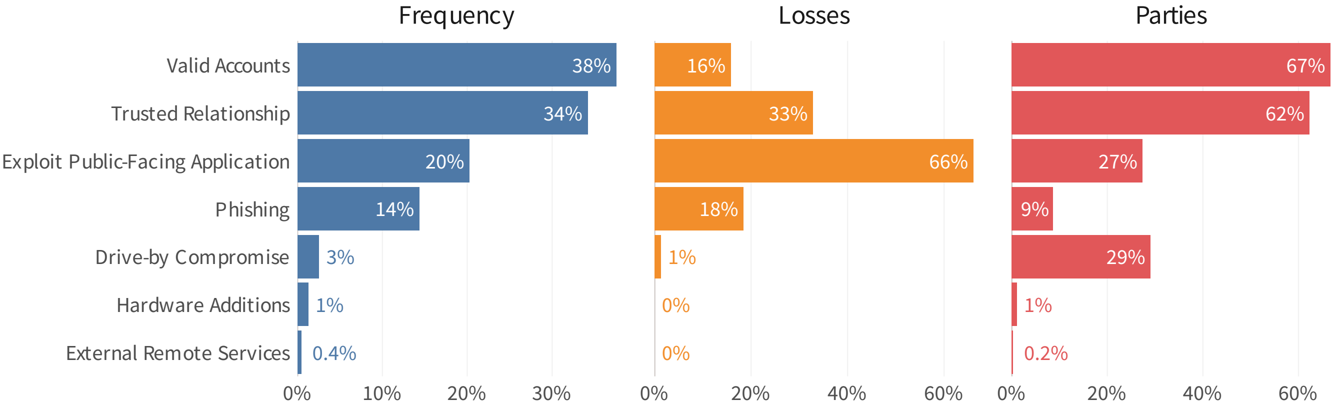
INITIAL ACCESS TECHNIQUES

Attackers use initial access techniques to gain entry to penetrate their target environment. From phishing to exploiting applications and supply chains, you're likely familiar with most of these techniques. Understanding initial access trends is crucial for identifying the best mitigations to ward off adversaries before they become deeply embedded in networks and systems.

> Among the most commonly employed initial access techniques, three of the four focus on exploiting trust: they either target trusted accounts or credentials, trusted associations with third parties, or rely on users who unknowingly engage with phishing schemes.

Recently, zero trust has become a huge topic in the cybersecurity industry of late, and looking at Figure 5, it's hard to argue against the core thesis of this strategy. Three of the four most frequent initial access techniques target trust—trusted accounts or credentials, trusted relationships with third parties, and trusting users who fall for phishing schemes. These techniques also rank in the top four for financial losses.

FIGURE 5: KEY STATS ASSOCIATED WITH THE INITIAL ACCESS TECHNIQUES USED IN RIPPLE EVENTS



The subversion of valid user accounts and trusted third-party relationships contribute to over 60% of downstream parties impacted by ripple events; and it's easy to see why. Once an attacker gains the privileges intended for trusted users or third parties, they're on the fast track to spreading across the network and supply chain. If you're curious about the underlying risk factors enabling this spread, our Balancing Third-Party Risk report offers useful insight.

The compromise of legitimate user accounts and established relationships with trusted third parties accounts for over **60%** of the organizations affected by the repercussions of ripple events.

Web application exploitation stands out as a significant avenue for initial access in ripple events, ranking **3rd** in frequency and contributing to almost two-thirds of the total financial losses incurred.

The exploitation of web applications is another major initial access vector for ripple events. Not only does this technique rank third on the frequency scale, it contributes to nearly two-thirds of all financial losses! At the risk of coming across as too salesy, this validates the critical importance of continual assessments to ensure that internet-facing devices are properly secured.

Top Initial Access Mitigation Strategies

As mentioned above, many of the most common and impactful initial access techniques target trusted accounts. Therefore, it's fitting that several of the top mitigation methods illustrated in Figure 6 focus on securing those accounts and credentials (e.g., M1018, M1026, M1027, and M1032).

Other effective strategies include segmentation (M1030), limiting access to network resources (M1035), and isolating or sandboxing applications (M1048). These approaches can effectively restrict adversaries who manage to exploit accounts or applications.

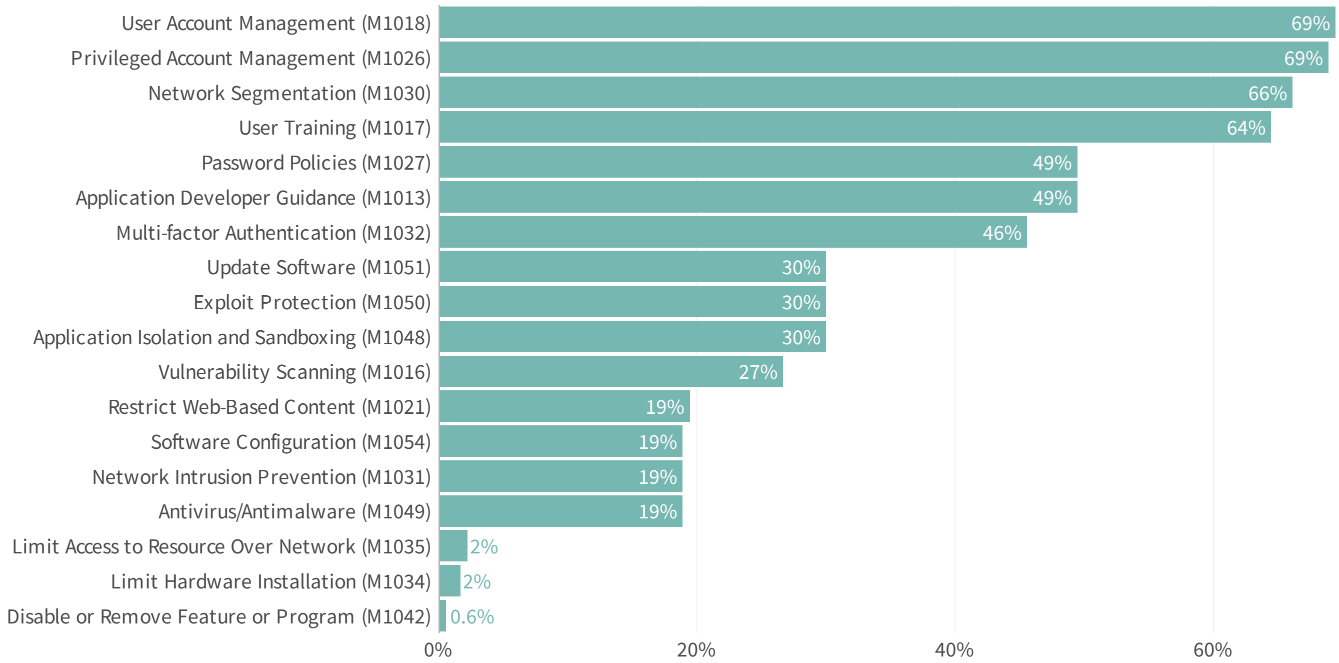


FIGURE 6: RECOMMENDED MITIGATIONS FOR THE MOST COMMON INITIAL ACCESS TECHNIQUES

Security hygiene emerges as a third theme woven through the recommended mitigations for initial access techniques. Implementing measures such as updating software (M1051), avoiding easy exploitation (M1050), conducting vulnerability scans (M1016), and restricting unnecessary web content and services (M1021) all reduce the likelihood of your organization falling prey to opportunistic attackers.

POST-COMPROMISE TECHNIQUES

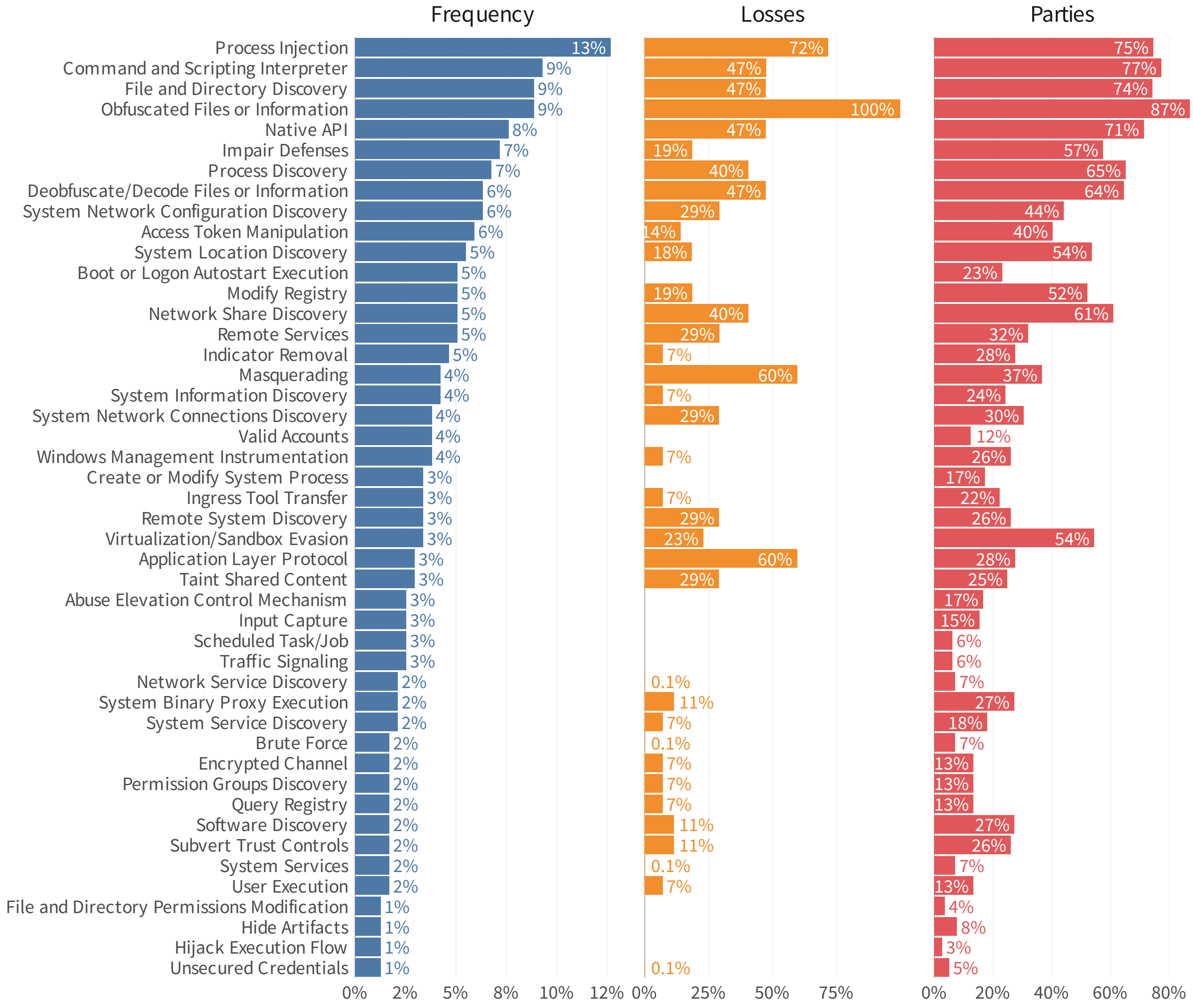
In the next portion of our research, we look at what attackers do once they have gained an initial foothold in the victim's central environment. These post-compromise techniques include all the illicit activities attackers do to maintain a presence, escalate privileges, spread across the internal network (and to connected third parties), evade security defenses, establish command and control channels, etc.

Figure 7 showcases all identified post-compromise techniques that contributed to at least 1% of ripple events. It's rather overwhelming—but that's actually a big part of the message we intend to convey. Attackers have an extensive toolkit at their disposal and use whatever is necessary to get the job done. Because the list is lengthy, we will highlight a few that stand out and leave the rest for your review at your leisure.

Process injection (T1055) is noteworthy, ranking #1 in frequency, second in financial losses, and third in affected downstream parties. Adversaries use this technique to introduce or execute malicious code within legitimate applications or services.

Speaking of introducing code, obfuscated files or information (T1027) constitutes another favored post-compromise technique. Attackers typically employ this method to deliver payloads without setting off alarms. Astonishingly, this tactic involved 100% of known financial losses and 87% of impacted parties in multi-party security incidents.

FIGURE 7: KEY STATS ASSOCIATED WITH TOP POST-COMPROMISE TECHNIQUES USED IN RIPPLE EVENTS



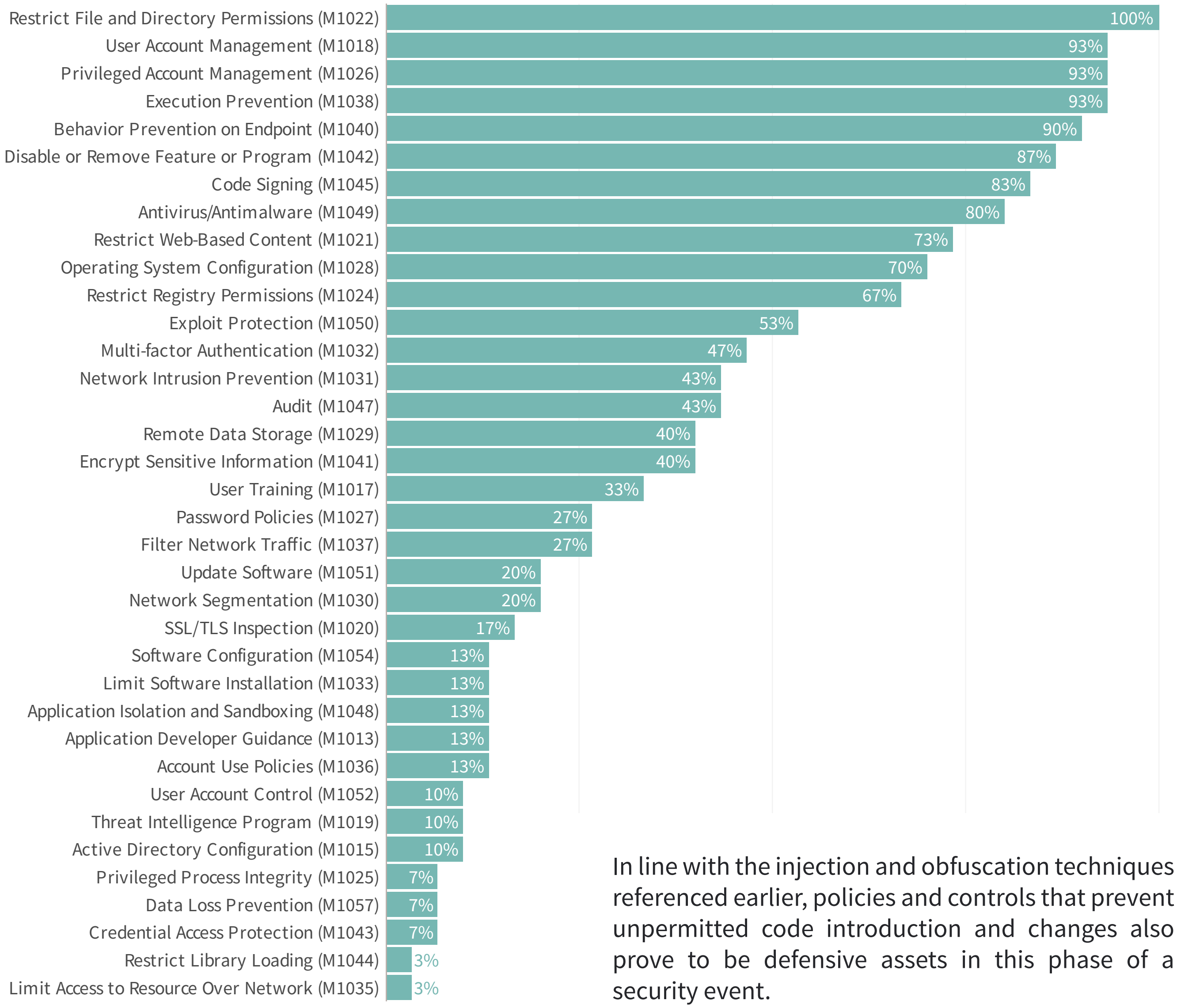
Masquerading (T1036) and application layer protocol (T1071) are even less common, but their association with over half of the financial losses warrants mention. The former technique involves disguising malicious activity or tools as innocent, and the latter is often used to blend in with legitimate traffic to evade detection.

Top Post-Compromise Mitigations

Given the extensive list of post-compromise techniques, it follows logically that the list of potential mitigations would also be considerable. Figure 8 doesn't disappoint in making this point.

Looking more closely, we see many of the same mitigation techniques also effectively thwart initial access attempts. That's good news, as it suggests things like managing accounts, restricting permissions, and hardening systems will pay double dividends for prevention and limiting the extent of the damage.

FIGURE 8: RECOMMENDED MITIGATIONS FOR THE MOST COMMON POST-COMPROMISE TECHNIQUES

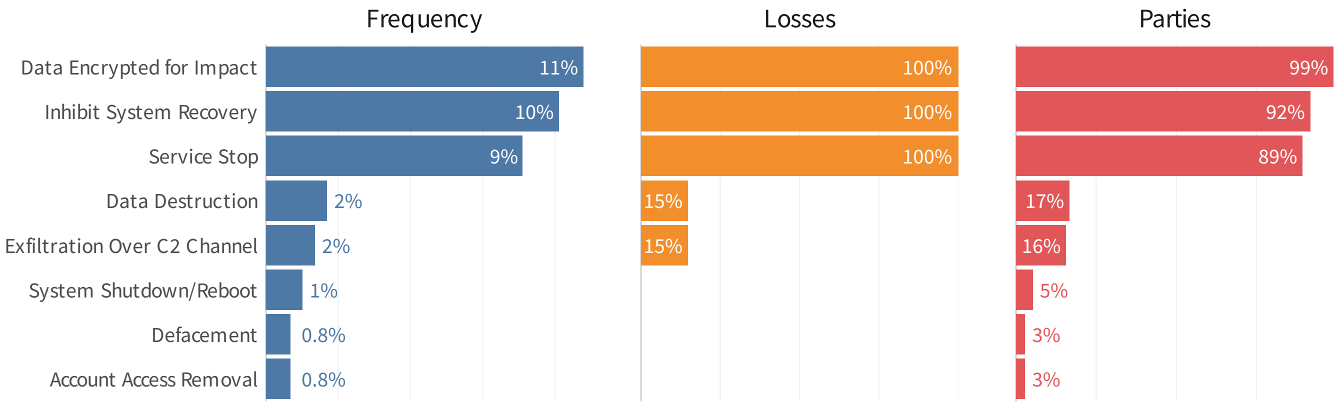


In line with the injection and obfuscation techniques referenced earlier, policies and controls that prevent unpermitted code introduction and changes also prove to be defensive assets in this phase of a security event.

DATA EXFILTRATION & IMPACT

Once attackers have the requisite depth and breadth of access into the environment(s), they will take action to achieve their ultimate goal(s). This generally involves exfiltrating data (TA0010) and/or negatively impacting systems (TA0040).

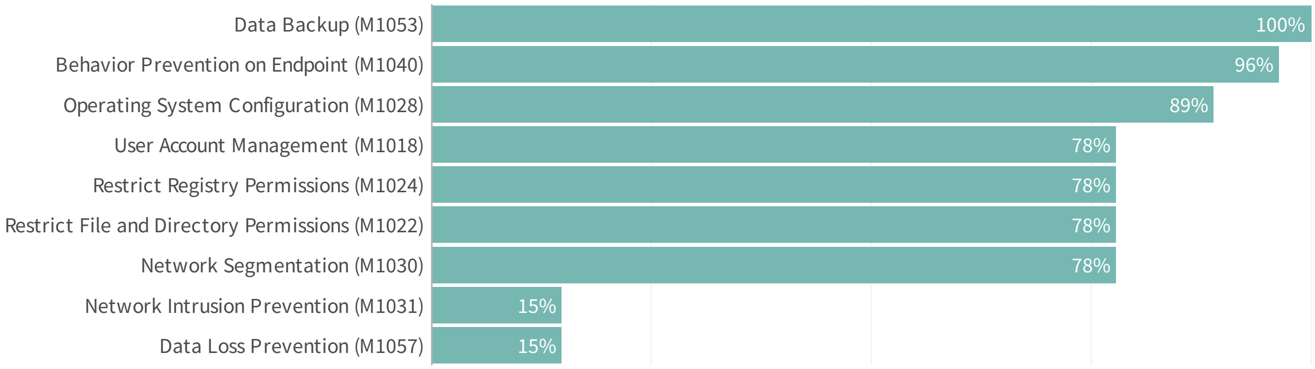
FIGURE 9: KEY STATS ASSOCIATED WITH TOP EXFILTRATION & IMPACT TECHNIQUES USED IN RIPPLE EVENTS



Top Exfiltration & Impact Mitigations

Accordingly, the mitigations that are likely to be most impactful at this stage include backing up data, further restricting permissions, and altering system configurations.

FIGURE 10: RECOMMENDED MITIGATIONS FOR THE MOST COMMON EXFILTRATION AND IMPACT TECHNIQUES

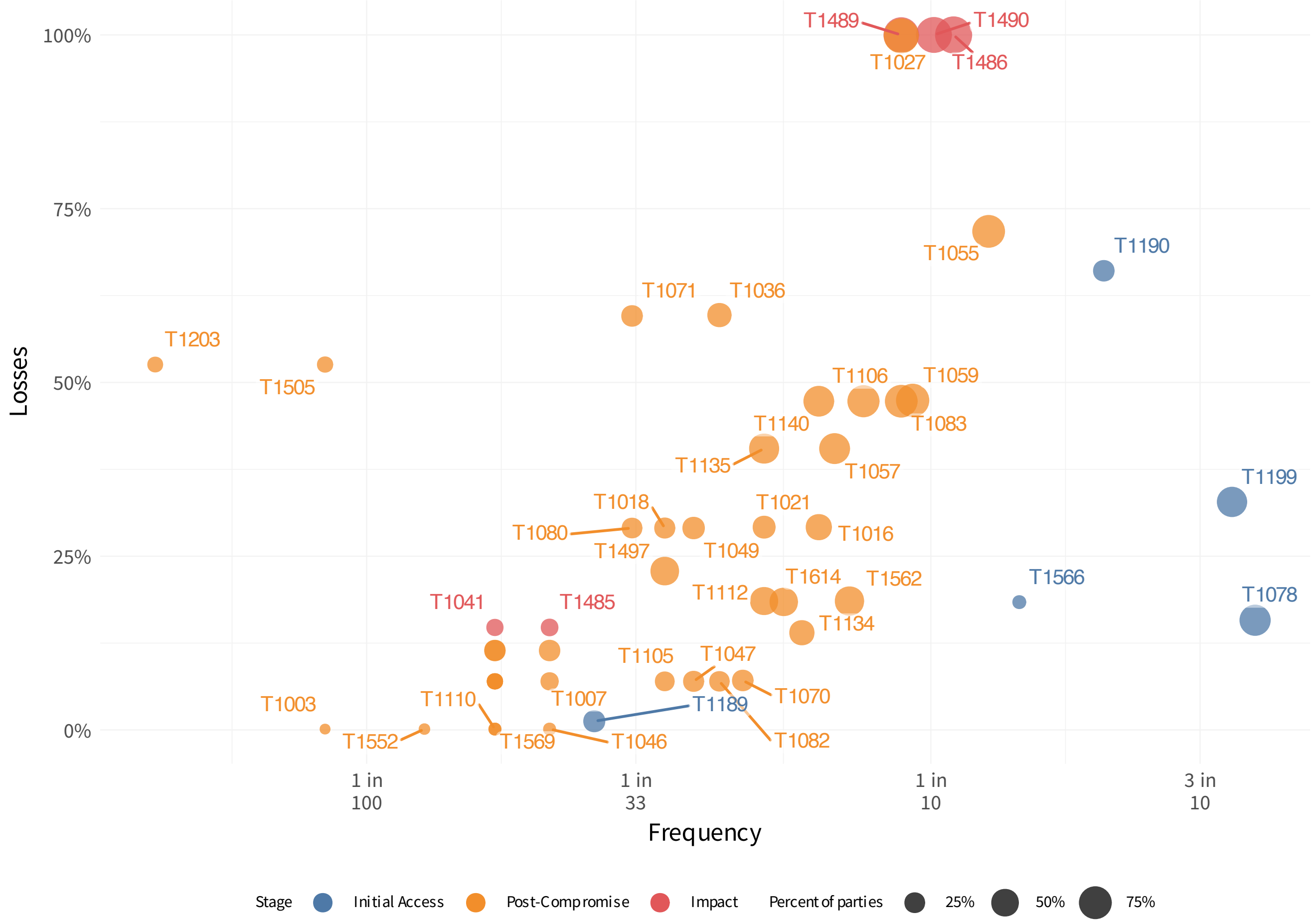


COMPARING KEY METRICS ACROSS ATT&CK TECHNIQUES

Breaking incidents down into major phases or tactic clusters, as we've done thus far, helps keep things focused and manageable. It's also helpful to zoom out and see the bigger picture - which is exactly what we'll do here.

The following chart compares the relative frequency (horizontal axis), financial losses (vertical axis), and the number of downstream parties impacted (size of dot) among ATT&CK techniques identified across all ripple events. We have also color-coded these techniques according to the tactic grouping in which they appear, whether it be initial access, post-compromise, exfiltration, or impact.

FIGURE 11: RELATIVE FREQUENCY, LOSSES, AND IMPACTED PARTIES FOR ALL ATT&CK TECHNIQUES IDENTIFIED IN RIPPLE EVENTS



We understand that you likely don't have the ATT&CK identifiers memorized, and including the full names for all of them would make this chart unreadable. To look them up, you can visit this site. Techniques are color-coded according to the phase in which they appear.

HERE ARE THE FOUR THAT FEATURE PROMINENTLY IN **HIGH FREQUENCY** AND **LOSSES**:

T1027: Obfuscated Files or Information

T1486: Data Encrypted for Impact

T1489: Service Stop

T1490: Inhibit System Recovery

Having already discussed these and many of the others in Figure 11 within their respective tactic groups above, we will not repeat that information here. However, we do hope that it assists your organization in quickly assessing which ATT&CK techniques represent the greatest risk for multi-party cyber events.

Top Overall Mitigations

By now, you recognize the pattern: we present techniques, and then we present their mitigations; however, it is not quite as simple when showing as many techniques as we have.

The chart below connects observed ATT&CK techniques to their potential mitigations. The size of the dot corresponds to how often each technique or mitigation was associated with an event. The connecting lines denote the strength of correlation between techniques and mitigations, with bolder lines indicating a stronger correlation.

You could attempt to follow the lines to identify all possible mitigations for techniques of interest; but, in honesty, this task would be much easier using MITRE's site. We chose this view because:

It portrays the complex, interconnected nature of defending against ripple events.

It reinforces the idea that multiple ways of mitigating the top ATT&CK techniques exist.

It demonstrates the possibility of defending against multiple techniques with a single mitigation.

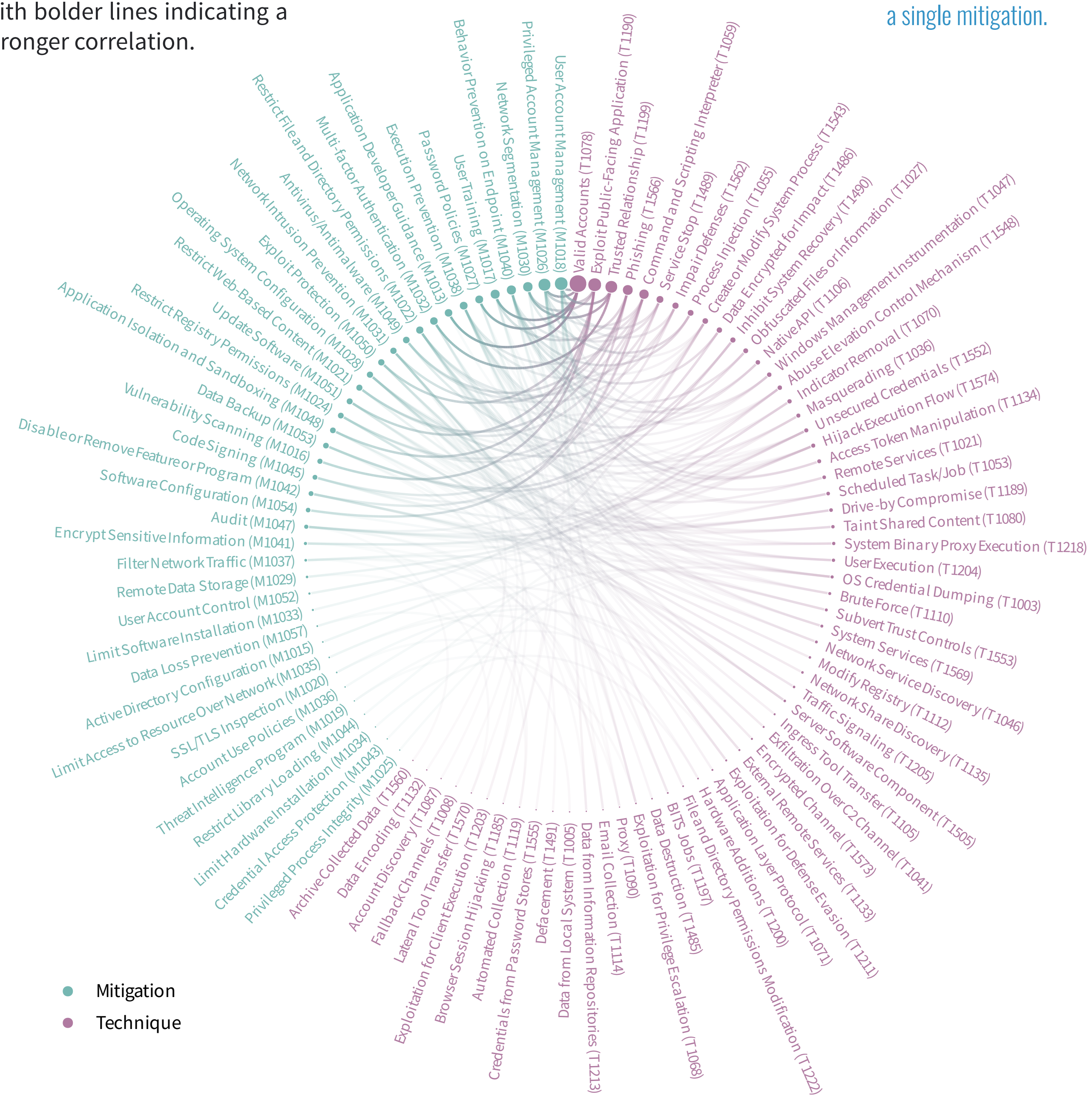


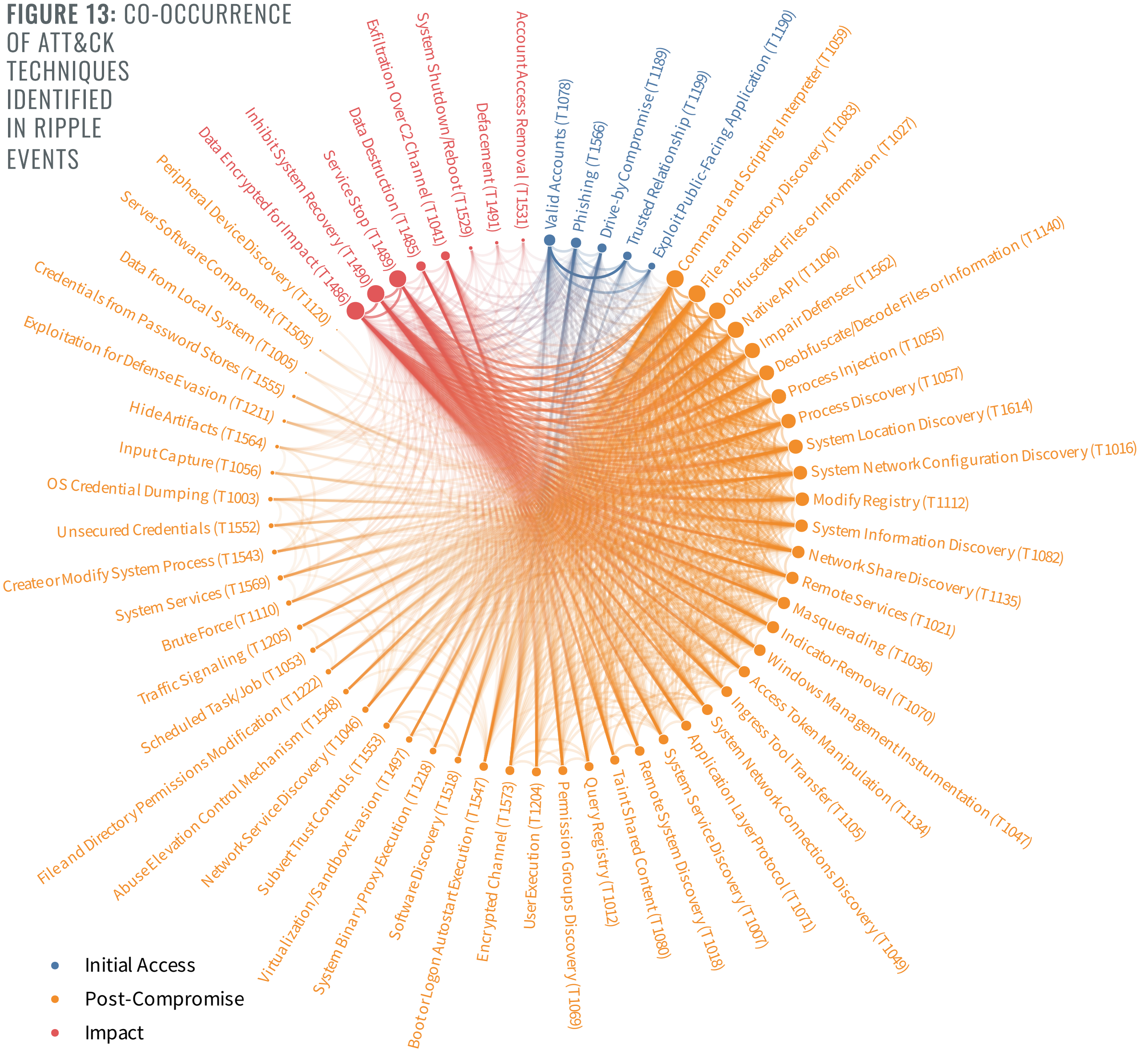
FIGURE 12: RECOMMENDED MITIGATIONS FOR TOP ATT&CK TECHNIQUES CONTRIBUTING TO RIPPLE EVENTS

TECHNIQUE CO-OCCURRENCE AND FLOW

There is one last concept we'd like to explore before concluding this report. Thus far, we have treated techniques as standalone actions. This approach is certainly useful for prioritizing defenses, but adversaries in real cyber attacks utilize a combination of TTPs in various, frequently recurring sequences – which is why tools such as ATT&CK Flow have been developed.

Using a sunburst chart, we'll begin with the concept of technique co-occurrence within events. This chart is even more interconnected than the previous one, so attempting to follow all the lines could be overwhelming. Nonetheless, it is essential to observe the multiple paths **within** and **between** the colored sections, which represent initial access (blue), post-compromise (orange), and exfiltration/impact (red) techniques.

FIGURE 13: CO-OCCURRENCE OF ATT&CK TECHNIQUES IDENTIFIED IN RIPPLE EVENTS



The frequent co-occurrence within initial access techniques, such as valid accounts (T1078) and Trusted Relationship (T1199), reflects the unique nature of ripple events. Multiple "initial" access points emerge as the incident spreads among victims.

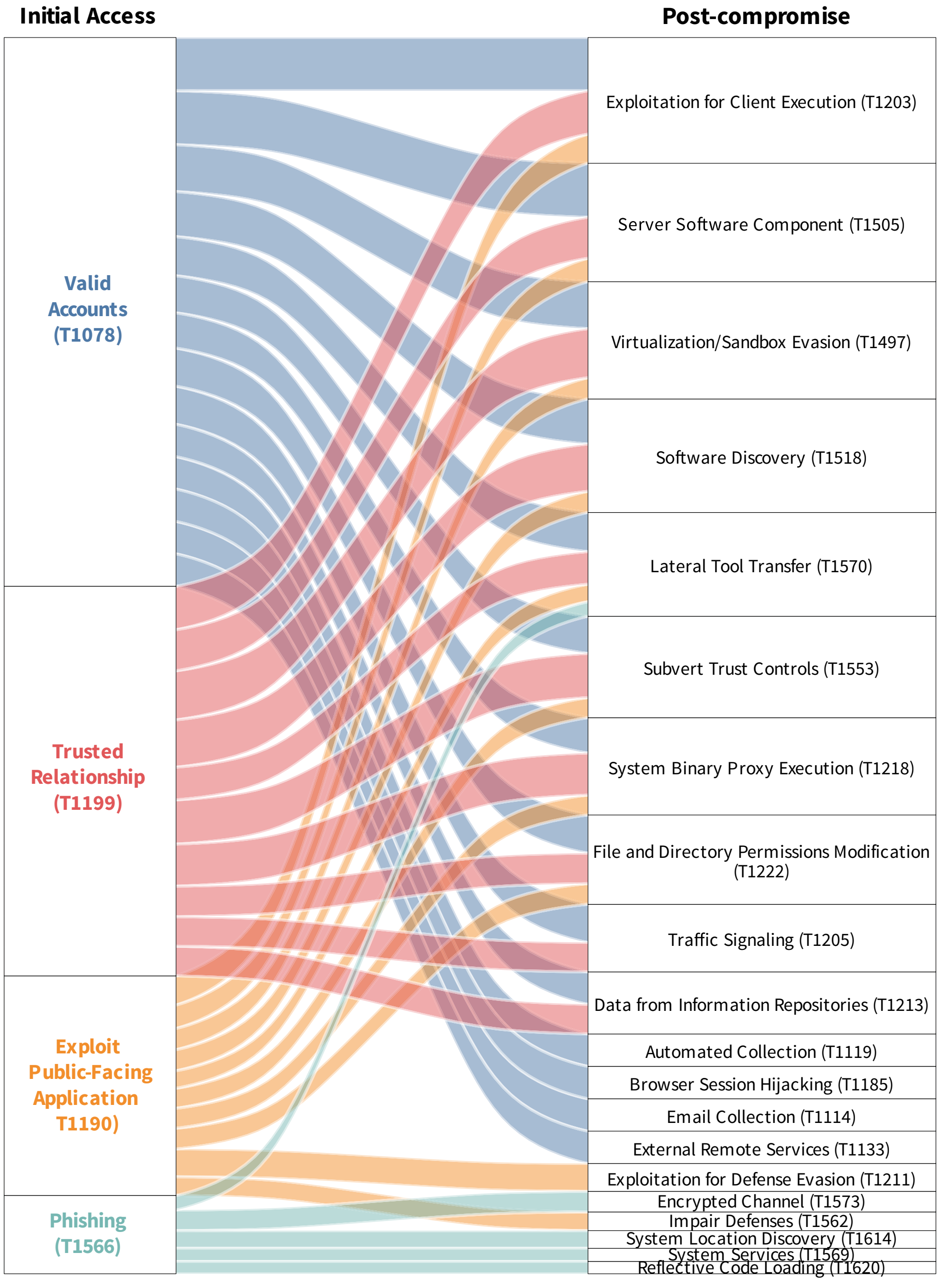
The myriad paths among post-compromise techniques reveal the "Swiss Army knife" nature of these incidents. Once inside the network (or supply chain), adversaries leverage whatever tools and methods move them toward their objective. Nevertheless, mitigating even one of these techniques — Command and Scripting Interpreter (T1059), for example — could still significantly disrupt the adversary's progression.

The connections between different tactic sets hint at technique combinations or flows that adversaries use to achieve their goals. If they always used the same sequence, there would be fewer, very prominent paths. The fact that we see more of a web-like structure suggests that adversaries do not follow a fixed script.

As an exercise in exploring inter-tactic flows, we mapped each of the top four initial access techniques to the post-compromise techniques most often observed following them. To simplify the tracking of these flows, we created the Sankey diagram, shown in Figure 14. Essentially, this diagram addresses the question, "After gaining access via a particular technique, what actions do adversaries tend to do after that?"

Overall, the message here is not one of "when attackers do x, they only do y." Some post-compromise techniques, such as those in the top half of the table, are versatile and accessible from a number of initial access techniques. Other post-compromise techniques are more clearly associated with specific initial access techniques, such as T1078 (Valid Accounts) or T1566 (Phishing).

FIGURE 14: FLOW BETWEEN INITIAL ACCESS AND POST-COMPROMISE ATT&CK TECHNIQUES IN RIPPLE EVENTS



CONCLUSION

A COMPREHENSIVE ANALYSIS OF MULTI-PARTY SECURITY INCIDENTS REVEALS SEVERAL SIGNIFICANT TAKEAWAYS.

Firstly, the financial ramifications of such incidents are notably higher, approximately seven times more costly, compared to single-party events. Among the various types of ripple events, system intrusions emerge as the most precarious, exhibiting both high frequency and substantial financial losses, impacting a multitude of third parties. The predominant methods of initial access involve targeting valid user accounts and leveraging trusted third-party relationships, underscoring the importance of robust authentication measures and diligent third-party management. Notably, exploiting public-facing applications contributes significantly to the financial toll of multi-party security incidents.

Surprisingly, incidents stemming from insider mistakes are not only twice as prevalent as those resulting from insider malice, but they are also exponentially more expensive, being 800 times costlier. Lastly, the involvement of malicious code injection and obfuscation is undeniably linked to reported financial losses, affecting 100% of cases, and impacting a substantial 87% of third parties in the context of multi-party security incidents. These findings emphasize the critical need for comprehensive security measures, vigilance in managing third-party relationships, and proactive strategies to mitigate the potential cascading effects of multi-party security breaches.

RiskRecon by Mastercard can play a pivotal role in addressing challenges related to third-party risk management and multi-party data breaches through its advanced capabilities and comprehensive approach:

Holistic Risk Assessment: RiskRecon offers a detailed and holistic assessment of third-party risk by continuously monitoring and evaluating the security posture of external partners. This proactive approach provides organizations with real-time insights into potential vulnerabilities and helps prevent security gaps that could lead to multi-party data breaches.

Vendor Ecosystem Visibility: RiskRecon enables organizations to gain a clear and comprehensive view of their entire vendor ecosystem. This visibility helps identify and prioritize high-risk vendors, allowing companies to focus resources on those most critical to their operations and security.

Prioritized Risk Scoring: RiskRecon employs automated risk scoring mechanisms custom-tuned to your business, in order to assess the security posture of your most important third parties. By assigning quantifiable risk scores, organizations can objectively compare and rank vendors, making informed decisions about their partnerships.

Continuous Monitoring: Multi-party data breaches often result from ongoing vulnerabilities in interconnected systems. RiskRecon's continuous monitoring capabilities ensure that vulnerabilities and risks are identified and addressed promptly, minimizing the potential for cascading breaches.

Mitigation Strategies: RiskRecon doesn't stop at risk assessment; it also provides actionable insights and recommendations for mitigating identified risks. This empowers organizations to take targeted measures to strengthen their own security as well as that of their third parties.

Compliance Management: Multi-party breaches can have legal and regulatory implications. RiskRecon aids organizations in maintaining compliance by identifying areas where third-party security practices may fall short of regulatory requirements.

Threat Prioritization: With its ability to identify the most impactful and likely risks, RiskRecon assists organizations in allocating resources effectively, focusing on the most critical vulnerabilities to prevent multi-party breaches.

RiskRecon offers a comprehensive and proactive approach to third-party risk management that is well-equipped to address the complexities of multi-party data breaches. By providing continuous monitoring, risk assessment, actionable insights, and a focus on vendor ecosystem visibility, RiskRecon helps organizations bolster their security measures and minimize the potential for multi-party breaches and their far-reaching consequences.

riskrecon by

RiskRecon enables clients to easily understand and act on their third-party risk through cybersecurity ratings and continuous security control assessments.

www.riskrecon.com

119 Cyentia INSTITUTE

The Cyentia Institute produces compelling, data-driven research with the aim of improving knowledge and practice in the cybersecurity industry.

www.cyentia.com