WEBINAR SUMMARY

January 28, 2021

Tapping on the Wire: Understanding Malicious Behaviors on the Network

Chris Derton, SE Manager, Rubrik
Karl Klaessig, Director of Product Marketing, Security Operations, ServiceNow
Veronica Valeros, Director of the Civilsphere project, Czech Technical University

KEY TAKEAWAYS

- Analyzing network traffic shifts the focus from the software to the attacker.
- Malware needs to communicate. That communication can be used to identify attacks.
- Rubrik provides the visibility necessary to recover quickly from malware attacks.
- ServiceNow's automated workflows enable teams to respond collaboratively.

in partnership with

OVERVIEW

Malware, on its own, is a piece of software that has the potential to be disruptive and destructive to the business. What it actually does, and when it does it, is ultimately determined by the attacker, a person with specific intentions and goals.

Analyzing network traffic enables defenders to not only see that the malware is on the network but understand what it is doing and the impact it has. Having the right tools in place can simplify not just identifying malware but remediating and recovering from it.

CONTEXT

Veronica Valeros discussed how analyzing network traffic allows defenders to better understand how attackers are using malware. Chris Derton and Karl Klaessig discussed how Rubrik and ServiceNow solutions work together to analyze network traffic to identify malware and automate response and recovery, improving the network's defense.

KEY TAKEAWAYS

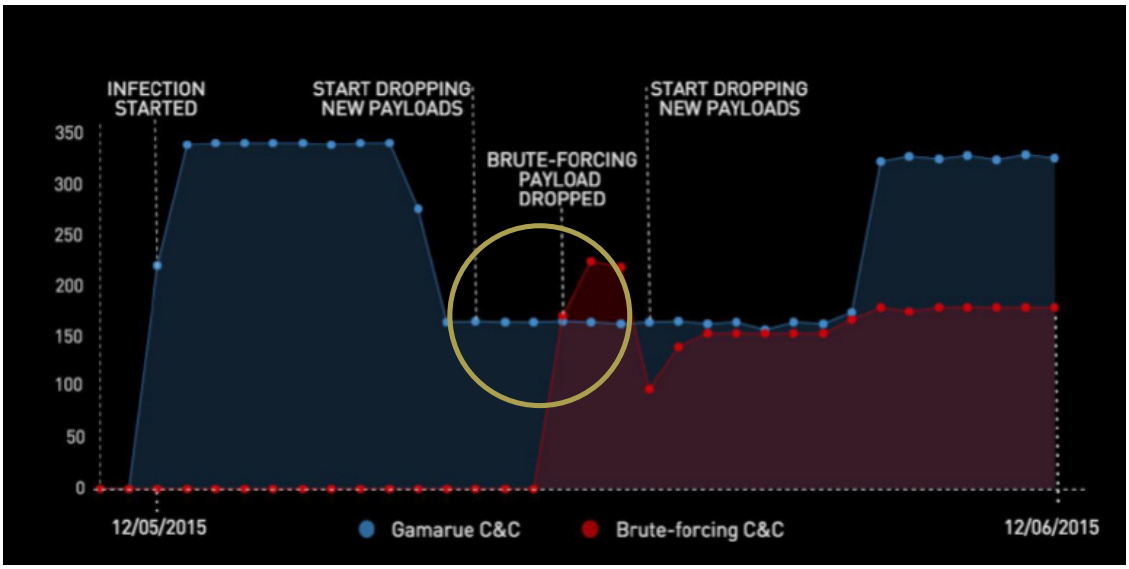
Analyzing network traffic shifts the focus from the software to the attacker.

Analyzing a piece of malware provides information on what the software has the potential to do, but not what it will do or when it will do it; those aspects are controlled by the human attacker. Tapping on the wire and looking at the network traffic shifts the focus from the malware to the attacker.

> Each decision of what the malware is going to actually do is taken by the attacker, who is a human with a purpose, with goals, with needs, and with a social context.
>
> *Veronica Valeros, Czech Technical University*

As seen in the below example, malware can sit on a system for some time before it begins to attack. The network traffic shows that the botnet checked in regularly, but the moment when the brute-forcing command and control payload was dropped onto the system was an unpredictable human decision. That moment is captured by the network traffic analysis.

Figure 1: Network traffic captured May 12 to June 12, 2015, shows the shift from infection to attack



Malware needs to communicate. That communication can be used to identify attacks.

Whether to grow and infect other machines on the network, to adapt, or to accomplish the goals of the person behind the attack, malware needs to communicate. Knowing what to look for in this communication can be used to identify attacks so they can be stopped and quickly remediated.

What to understand when analyzing network traffic for malware	
The behavior of users	Create a baseline of normal network traffic based on user behavior.
The baseline	Review the baseline of normal network traffic, including factors that change the baseline pattern, such as location, department, and even day of the week.
Who is being targeted	Identifying who is the target of an attack—the users or the organization—can help narrow down what should be looked at when analyzing traffic.

When identifying attacks, some visibility is better than no visibility. Organizations with limited budgets can still perform basic network monitoring to uncover potential problem areas.

Rubrik provides the visibility necessary to recover quickly from malware attacks.

Many malware attacks today are ransomware attacks. The lack of visibility into the scope of damage done by these attacks is one reason why the FBI expects organizations to pay out more than $1 billion in 2021.

Why organizations are paying ransom

- **Lengthy downtime.** Forrester says the average recovery time is 7.3 days.
- **Inability to recover.** Ransomware isn't just targeting the original data; it is targeting online backups, encrypting them, or completely deleting them.
- **Lack of visibility into the scope of the damage.** It is difficult to roll back the system when it is unclear what the complete blast radius was.

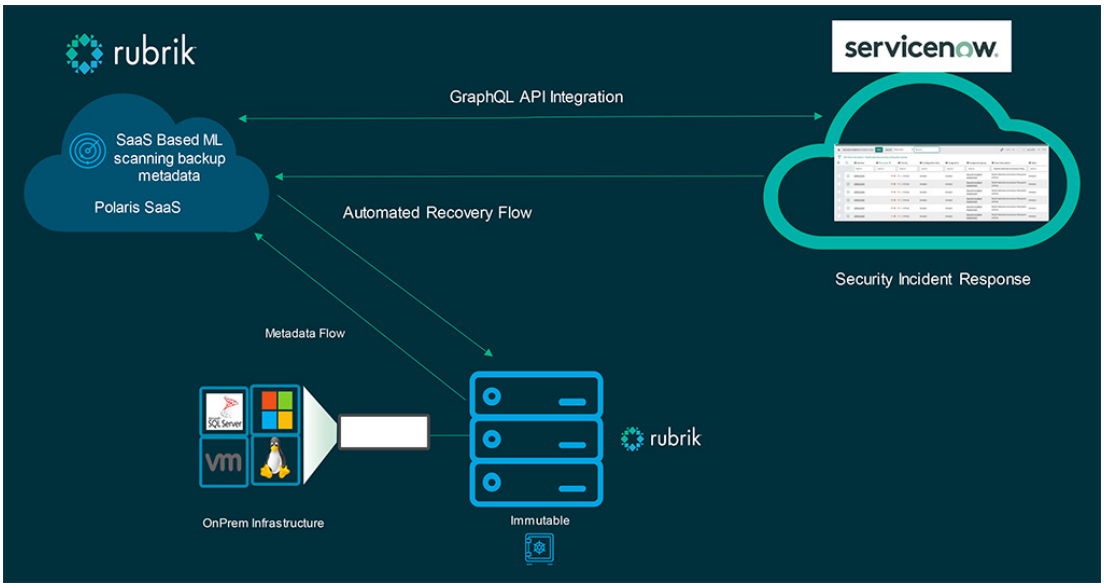
> When you get hit, there's a lengthy downtime with today's solutions. That downtime is just not ok for most customers. They know that their business is going to be impacted massively.
>
> *Chris Derton, Rubrik*

Rubrik provides the visibility that companies need, enabling businesses to quickly detect an attack, assess the damage, and recover without having to pay the ransom. Rubrik's Polaris software-as-a-service (SaaS) solution accelerates and simplifies recovery. Rubrik's solution:

- **Identification of abnormal behavior** on existing backup data, using machine learning (ML). This information can be shared with automation frameworks and security incident response solutions, such as ServiceNow.
- **Granular impact assessment** of the blast radius, offering a clear view of the files that were impacted.
- **Immutability and instant recovery;** since Rubrik data is never available in read/write mode, it can't be overwritten. One-click recovery quickly restores the system to the most recent, clean version.

Rubrik Polaris SaaS includes an automated ransomware detection and remediation solution—Polaris Radar—which uses ML to analyze snapshots of on-premise metadata, learn behavior patterns, and then identify ransomware attacks. Via application programming interface (API) integration, this information is shared with automation frameworks, like ServiceNow.

Figure 2: Rubrik Polaris SaaS integrates with ServiceNow to drive an automated recovery workflow



ServiceNow's automated workflows enable teams to respond collaboratively.

IT and security teams need to work collaboratively to address security issues and attacks, but most don't have the tools and resources in place to prioritize and respond to incidents quickly.

ServiceNow's security incident response solutions address the major challenges these teams face when responding to attacks.

Challenges facing IT and security teams under attack

- **No context.** 76% of organizations have no common view of assets and applications across security and IT.
- **Few resources.** 82% of employers report a lack of cybersecurity skills.
- **Manual processes.** 56% say things slip through the cracks because emails and spreadsheets are used to manage response processes.
- **Silos.** 62% of breached organizations were unaware that their organizations were vulnerable to a breach.

> Threats move at machine speed. Automating these processes and workflows is more valuable than ever because you need to move quickly to prevent these incidents from impacting your business.
>
> *Karl Klaessig, ServiceNow*

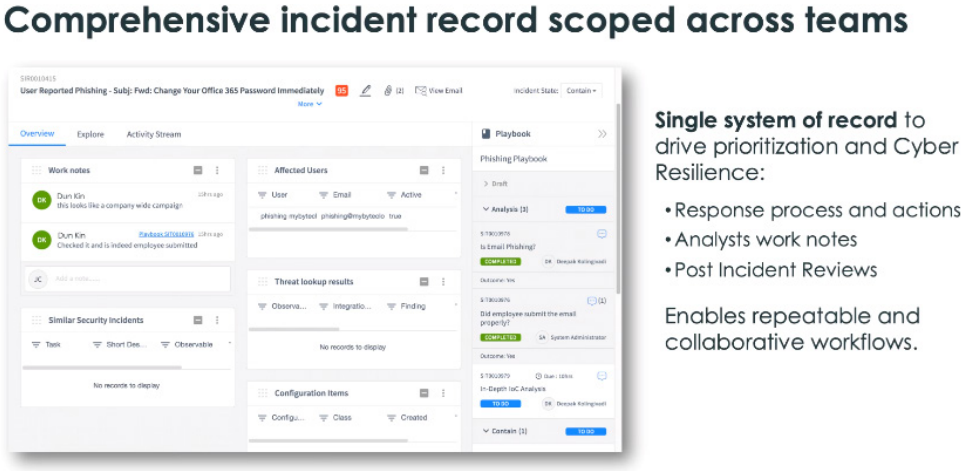
Automating incident response through ServiceNow enables organizations to:

- **Effectively manage** the evolving threats to the business.
- **Proactively manage** exposure and ensure cyber-resilience by establishing an effective and repeatable process.

- Drive efficiencies, not only accelerating reaction and response time, but enabling organizations to respond with existing teams and resources.

ServiceNow provides a single, comprehensive incident record that includes information, including ransomware attacks detected by Rubrik, necessary to drive prioritization and efficiencies across the teams. Workflows, orchestration, and automation are used to route work seamlessly between security and IT teams, to ensure a quick and efficient solution and centralize real-time status and reporting. As part of that response, Rubrik can be used to recover data from its protected backups, as necessary.

Figure 3: ServiceNow provides a comprehensive incident record scoped across teams



BIOGRAPHIES

Chris Derton

SE Manager, Rubrik

Chris Derton is currently the Rubrik Systems Engineering Manager for the TOLA region. He leads a team of pre-sales engineers focused on modern, scalable data management platform solving challenges with data security, cloud mobility, and application availability. Prior to joining Rubrik 3 years ago, Chris held pre-sales and pre-sales leadership roles for companies focused on data center architecture, SaaS delivered business continuity solutions, and hyperconverged software solutions.

Karl Klaessig

Director of Product Marketing, Security Operations, ServiceNow

Karl is ServiceNow's Director of Product Marketing, Security Operations, and has over 15 years of experience in product positioning and marketing of enterprise security platforms, including SIEM, SOAR, and endpoint technologies, most recently from product marketing roles at RSA and McAfee, where he was responsible for the positioning of their security operations and automation platforms.

Veronica Valeros

Director of the Civilsphere Project, Czech Technical University

Veronica Valeros is a senior researcher and intelligence analyst from Argentina. Her research strongly focuses on helping people. She currently specializes in threat intelligence, malware traffic analysis, and data analysis. She has presented her research at international conferences such as Black Hat, EkoParty, Botconf, Virus Bulletin, Deepsec, and others. She is the co-founder of the MatesLab hackerspace based in Argentina and co-founder of the Independent Fund for Women in Tech.

She is currently the director of the Civilsphere project at the Czech Technical University, dedicated to protecting civil organizations and individuals from targeted attacks. She's also the project leader at the Stratosphere Laboratory, a research group in the Czech Technical University dedicated to study and research in cybersecurity and machine learning.