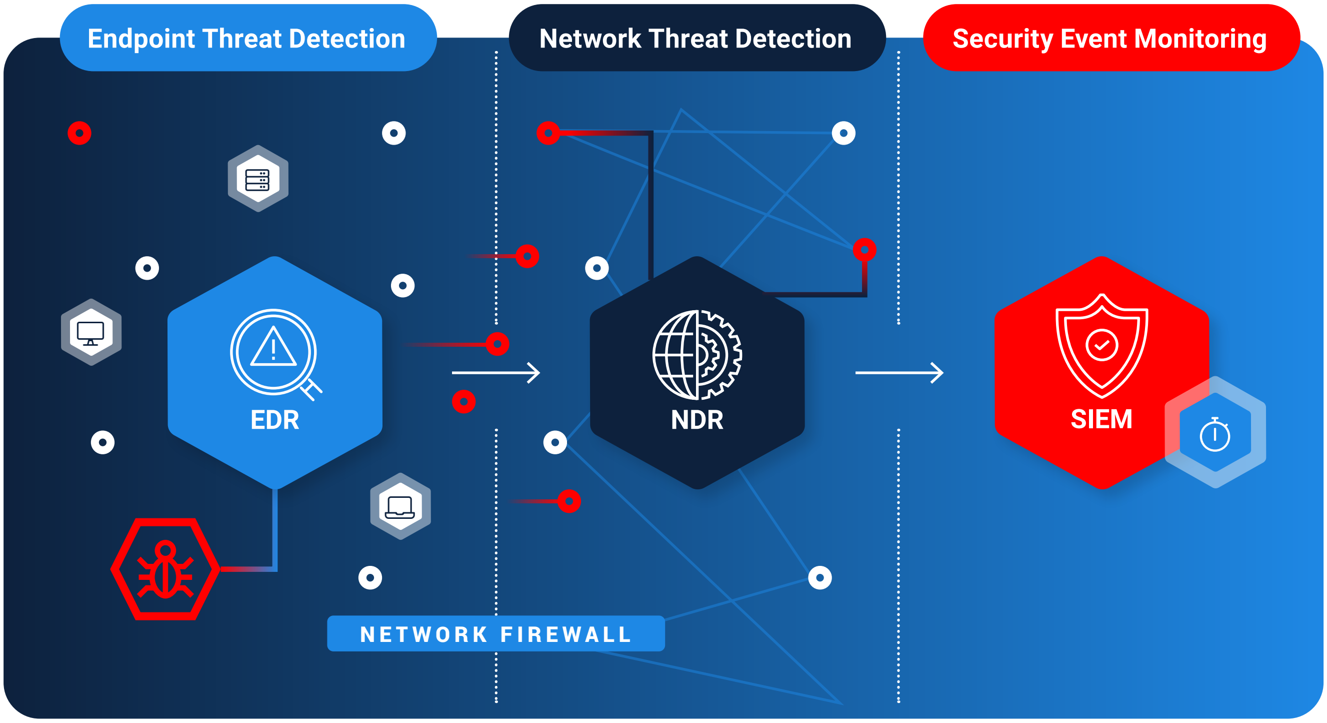
Catching ransomware campaigns before an attacker reaches their endgame

Why IronNet's network detection and response (NDR) capabilities are an essential component of your layered security strategy for preventing ransomware attacks

The key to catching ransomware is early detection at the network gate

Deployment of ransomware is not an instantaneous process. Instead, it is an indication that the network has been compromised through a series of events that have allowed the adversary to infiltrate the network, navigate through it, and eventually deploy the ransomware payload to set up the path for exfiltration and extortion.

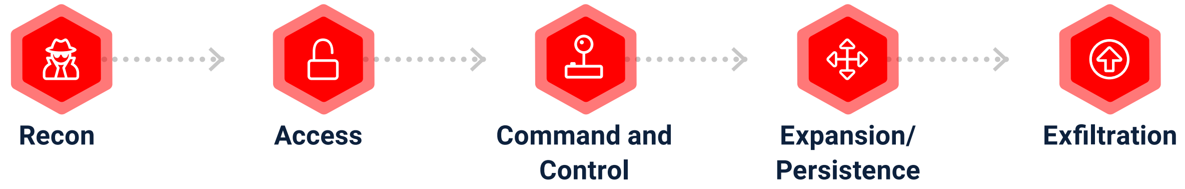


Network detection and response tools can detect threats that slip past endpoint detection tools and the firewall.

While ransomware itself is not a network-based attack, it is the host-based result of a network attack.

In other words, ransomware is the very last step an attacker takes after fully compromising a network to monetize their efforts.

These attacks are always enabled by network connectivity to some degree: delivery, lateral movement/spreading, command-and-control (C2), etc. Early detection of the initial network intrusion, therefore, is crucial, before the adversary has the chance to advance the ransomware campaign.



Detection at the early stage of intrusion is critical for mitigating ransomware's impact.

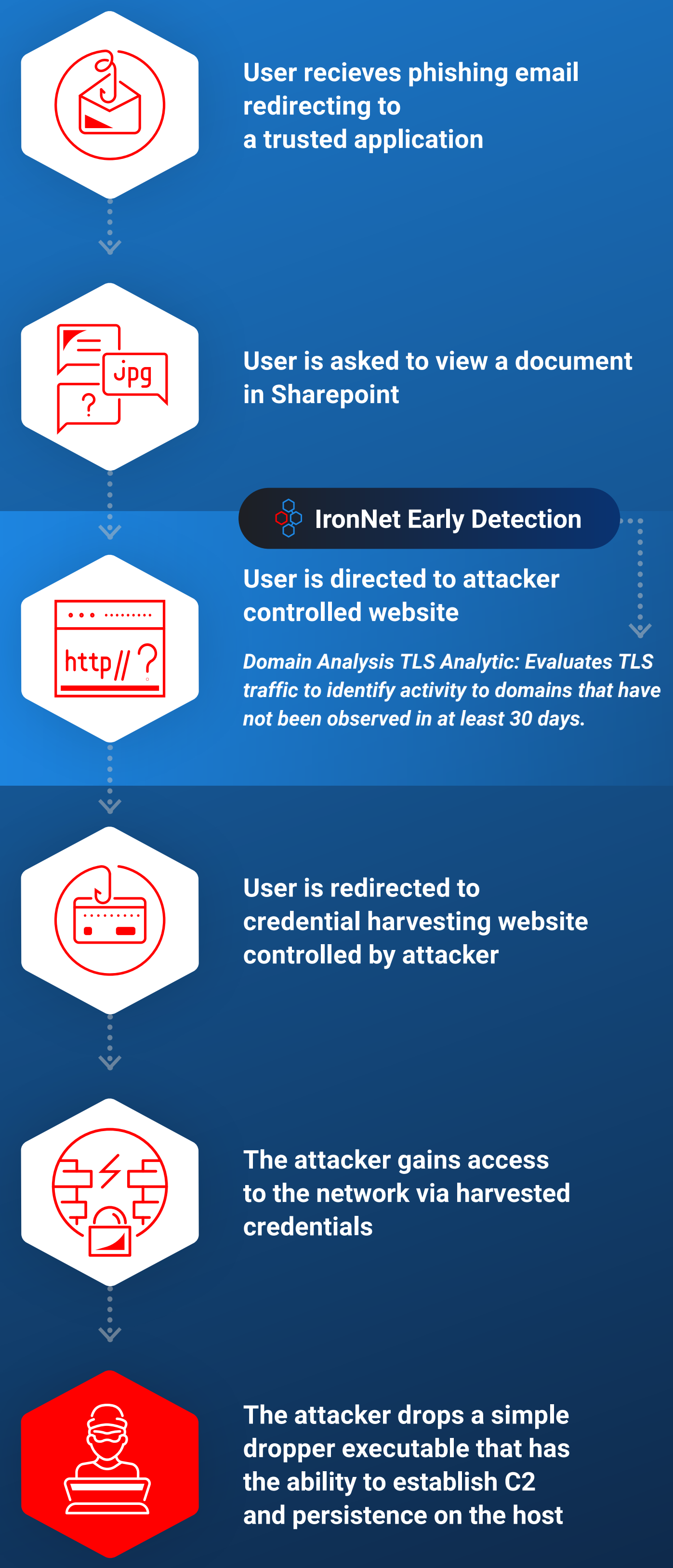
How do attackers launch a ransomware campaign?

Ransomware can spread through various social engineering techniques such as tricking users with phishing emails containing malicious attachments and links, redirecting them to malware-infected websites, asking them to install a fake software update, or by persisting within inadequately defended networks.

Based on typical ransomware TTPs, phishing remains the most common infection vector, whether conducted by APTs, sophisticated criminal groups, or script kiddies or delivered via adware. Phishing is most often in the form of a malicious document attached to an email or a link that aims to gather corporate credentials for remote access, a.k.a. “credential phishing.”

Attackers most often download additional payloads/modules as they spread from the compromised server down into the network, presenting further opportunity for detection of anomalous activity on the network itself. From there, the ransomware campaign unfolds.

An example of detecting phishing at the early stages of a ransomware campaign



User recieves phishing email redirecting to a trusted application

User is asked to view a document in Sharepoint

IronNet Early Detection

User is directed to attacker controlled website

Domain Analysis TLS Analytic: Evaluates TLS traffic to identify activity to domains that have not been observed in at least 30 days.

User is redirected to credential harvesting website controlled by attacker

The attacker gains access to the network via harvested credentials

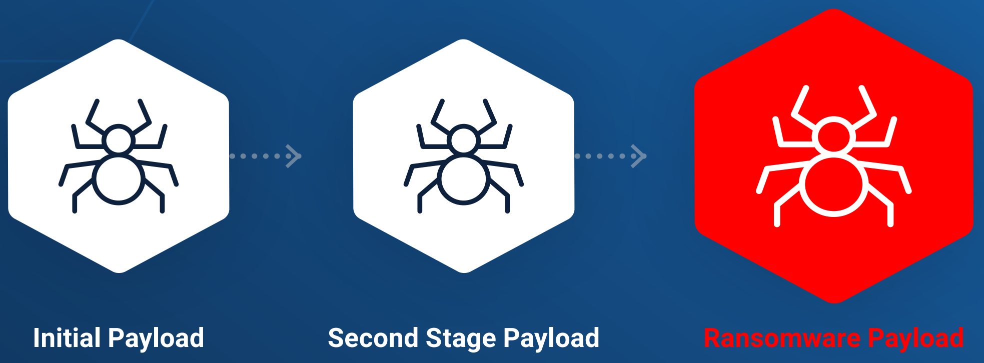
The attacker drops a simple dropper executable that has the ability to establish C2 and persistence on the host

How does an attacker successfully deliver ransomware after phishing a user?

The infection vector typically is a simple dropper executable, often delivered via email, that has the ability to establish C2 and persistence on the host. This initial access mechanism is, by design, rarely sufficient so attackers most often download additional payloads/modules as they spread from the compromised server down into the network, presenting further opportunity for detection of anomalous activity on the network.

The actual delivery of the ransomware payload is typically separate from the initial payload or even the second-stage payloads used to move around the network. This is because attackers have learned to deploy only final stage payloads when needed in order to avoid detection/analysis.

Because IronNet behavioral analytics can detect campaigns at all these stages of network intrusion, IronNet's network detection and response (NDR) solution, IronDefense, is an important part of a defense-in-depth security strategy in the fight against ransomware.



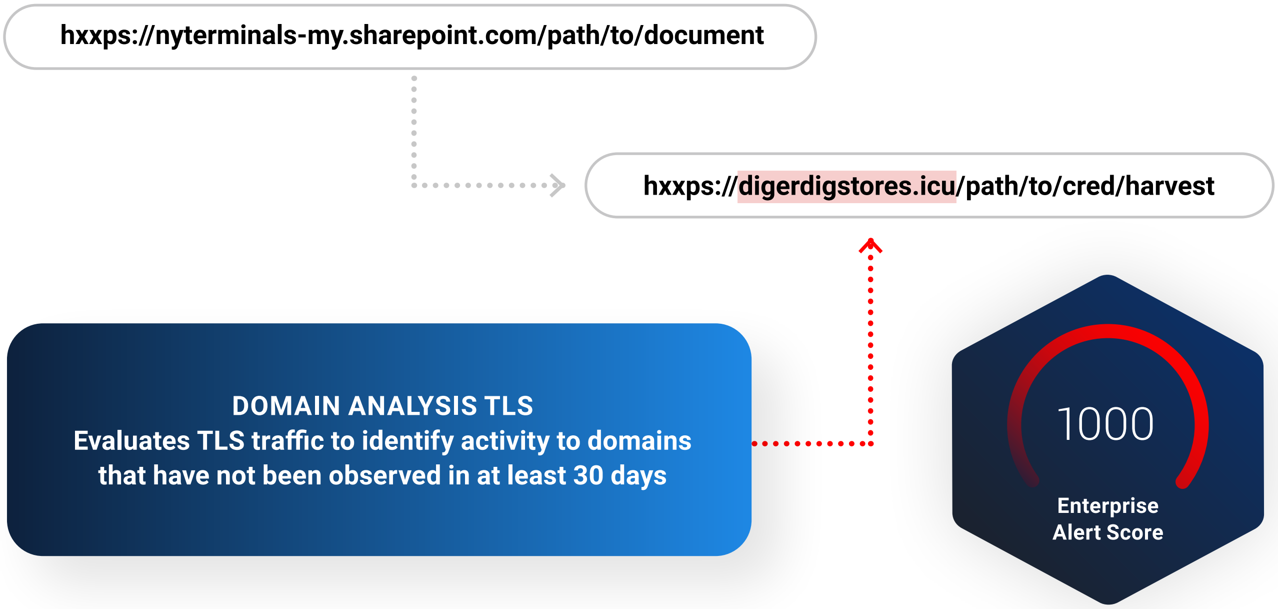
How do IronNet behavioral analytics detect phishing?

Attackers have gotten quite good at gathering intelligence on how organizations operate to give their phishing emails more legitimacy to bypass automatic detection/blocking as well as human identification. Additionally, compromises in email services such as Constant Contact can give an attacker the ability to avoid most traditional email-based detection mechanisms.

As an advanced NDR solution, **IronDefense** leverages proprietary behavioral analytics to spot anomalies and detect malicious behaviors on networks. IronNet's Suspicious File Downloads, Phishing HTTPS, Credential Phishing, PII Data Loss analytics, and Domain Analysis TLS analytics, for example, can detect these edge cases not covered by training or email inspection/sandbox solutions.

Defense-in-depth detections

What's more, IronNet's analytics are not isolated to just email-based phishing detections; they also identify any time a user appears to be interacting with a phishing link or submitting sensitive information to a suspicious external entity. It is common for defenders to look at phishing only in the context of email, but there are a number of ways a user could stumble on a phishing page (instead of launching the attack via an email), such as watering hole attacks, social media, malicious advertisements, SEO manipulation, etc.



hxxps://nyterminals-my.sharepoint.com/path/to/document
hxxps://digerdigstores.icu/path/to/cred/harvest

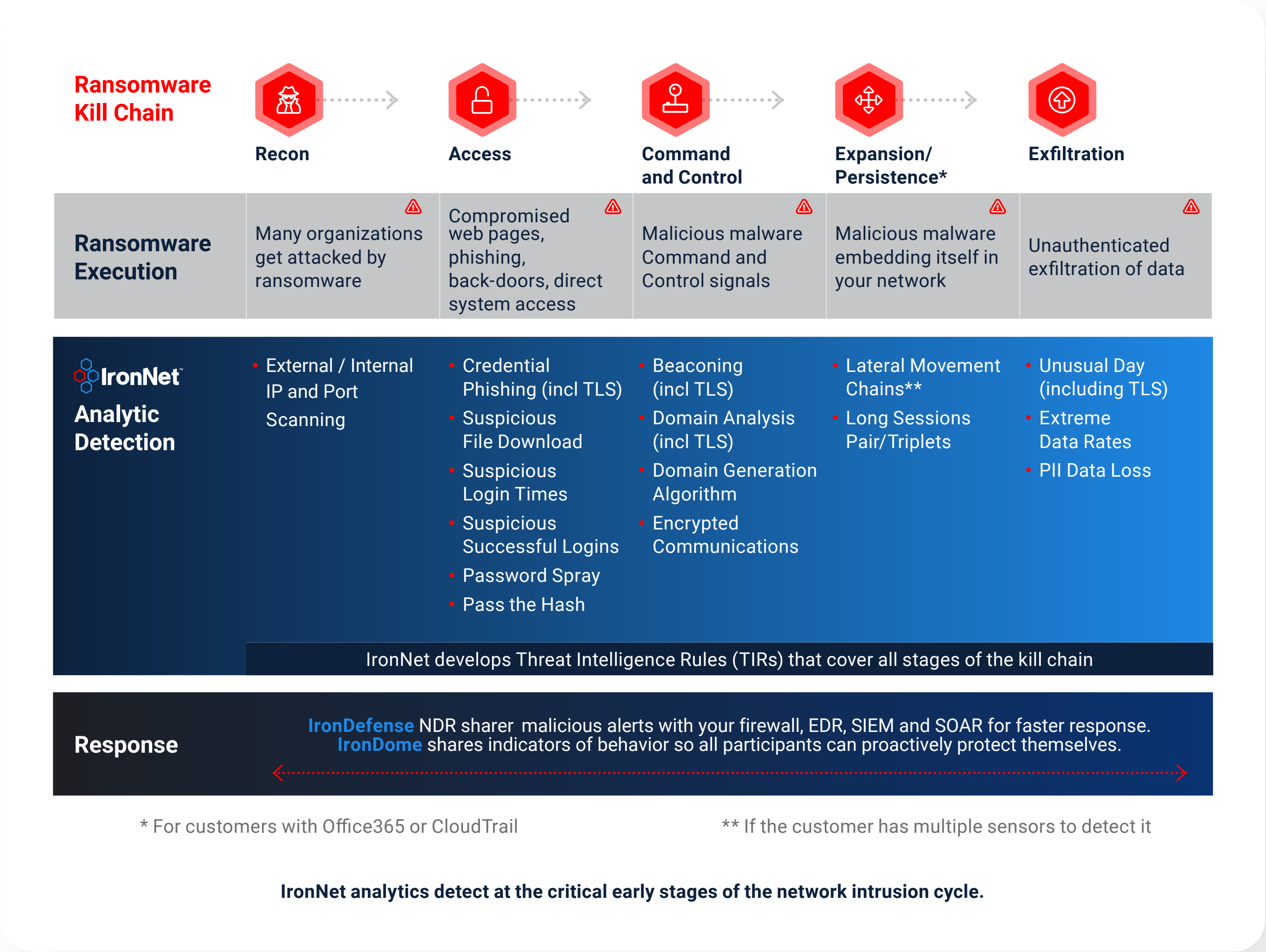
DOMAIN ANALYSIS TLS
Evaluates TLS traffic to identify activity to domains that have not been observed in at least 30 days

1000
Enterprise Alert Score

An example of how the IronNet Domain Analysis TLS analytic detects and alerts at a high severity score.

How does ransomware advance across the network?

Once a target network has been identified, the adversary starts launching the attacks that will gain them an initial foothold into their victim's network. After the perimeter has been breached, the adversary will normally undergo a silent period of observation and data gathering. Their objective at this stage is to learn as much as possible about your enterprise network and your users, collecting user names and passwords, escalating privileges, and deploying toolkits that will be required in the later stages of the ransomware attack.



Ransomware Kill Chain	Recon	Access	Command and Control	Expansion/ Persistence*	Exfiltration
Ransomware Execution	Many organizations get attacked by ransomware	Compromised web pages, phishing, back-doors, direct system access	Malicious malware Command and Control signals	Malicious malware embedding itself in your network	Unauthenticated exfiltration of data
IronNet Analytic Detection	• External / Internal IP and Port Scanning	• Credential Phishing (incl TLS) • Suspicious File Download • Suspicious Login Times • Suspicious Successful Logins • Password Spray • Pass the Hash	• Beaconing (incl TLS) • Domain Analysis (incl TLS) • Domain Generation Algorithm • Encrypted Communications	• Lateral Movement Chains** • Long Sessions Pair/Triplets	• Unusual Day (including TLS) • Extreme Data Rates • PII Data Loss

IronNet develops Threat Intelligence Rules (TIRs) that cover all stages of the kill chain

Response

IronDefense NDR sharer malicious alerts with your firewall, EDR, SIEM and SOAR for faster response.
IronDome shares indicators of behavior so all participants can proactively protect themselves.

* For customers with Office365 or CloudTrail

** If the customer has multiple sensors to detect it

IronNet analytics detect at the critical early stages of the network intrusion cycle.

This is another crucial phase for leveraging IronNet's behavioral analytics to spot the attacker early in their campaign. IronNet has built a large portion of our behavior analytics to actively detect behavioral indicators that relate to a ransomware attack.

3 levels of extortion to increase the ransom

In its current form, ransomware is the end result of intensive manual enumeration and exploitation of Active Directory infrastructures, typically involving full domain compromise where an attacker has escalated privileges and access to a point where they are able to disseminate their malware to any compatible host/server. Attackers do not stop there, however.

We are now seeing a new way to increase payments through what defenders are referring to as "double extortion" or "triple extortion." Double extortion is simply the act of exfiltrating the data that is targeted for encryption and threatening to leak the sensitive data if the company does not pay the ransom. Triple extortion is slightly more involved and refers to the threat actor analyzing the exfiltrated data for potentially sensitive customer data — such as medical records — and reaching out directly to the third-party, demanding payment based on the threat of leaking their personal details.

While truly stopping ransomware, which fundamentally is an attack on an endpoint, requires some level of endpoint visibility or control (as enabled by endpoint detection vendors such as CrowdStrike), IronNet can help detect the malicious activity associated with ransomware — in other words, the activity in virtually every case that precedes the encryption and exfiltration of data, therefore preventing ransomware from ever reaching our customers' enterprise networks.

Triple Extortion

DDoS

Double Extortion

Exfiltration

Single Extortion

Encryption

Breaking the ransomware chain: 4-step protection with IronNet

1 Detecting early ransomware activity using network behavior analytics

IronNet's behavioral analytics detect anomalies early in the ransomware lifecycle, during the intrusion vectors and network dwell time, sounding alerts to halt this type of progression.

Case study: Mapping IronNet analytics to DarkSide's ransomware toolkit (as cited from Sophos)

Initial Access	Execution	Defense Evasion	Discovery	Persistence	Lateral Movement	Exfiltration	Impact	Command & Control
⬡ Phishing of credentials	⬡ Cobalt Strike	Powertool64	ADRecon	\Windows\System32\net.exe	⬡ PSExec	Mega.nzpCloud	wwifi.exe (ransomware executable)	Plink
⬡ External remote access (VPN,RDP)	PSExec	PCHunter	ADFind	GPO	⬡ Remote Desktop Protocol	⬡ puTTy	azure_update.exe	⬡ AnyDesk
	SystemBC	GMER	⬡ NetScan	Scheduled Tasks	⬡ SSH	Rclone		⬡ Cobalt Strike
			Advanced IP Scanner			7zip		

In the specific case of the toolkits used by the DarkSide ransomware group to launch and execute their ransomware attacks, IronNet's behavioral analytics would have detected their attack at various points in the kill chain, giving Infosec teams a good chance to respond to the threat before DarkSide reached their endgame.

2 Proactive protection with IronNet threat hunting and data scientist insights

IronNet threat hunters proactively search for unknown threats on the network to spot adversaries that have slipped past firewalls and endpoint detection tools to lurk in networks, scoping the environment for the perfect opportunity to pounce with their ransom demands. Working with data scientists, IronNet threat hunters fine-tune behavior analytics through regular software updates to automatically rate the severity of network threats, in turn enabling faster response.

Case study: LockBit Ransomware

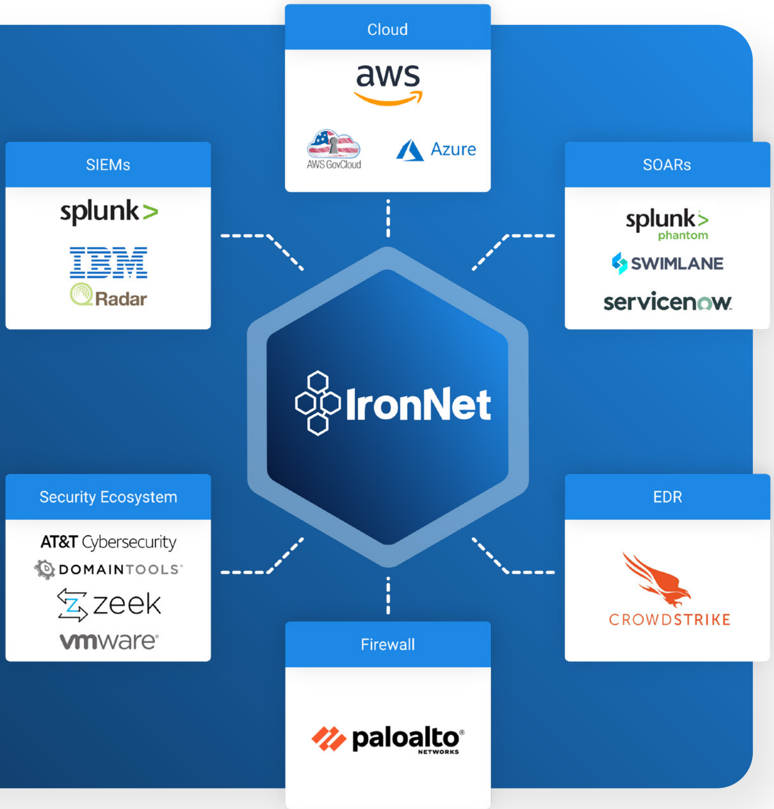
Swiss cyber threat intelligence company PRODAFT recently released an **in-depth analysis on LockBit ransomware-as-a-service (RaaS)**. IronNet hunting insights:

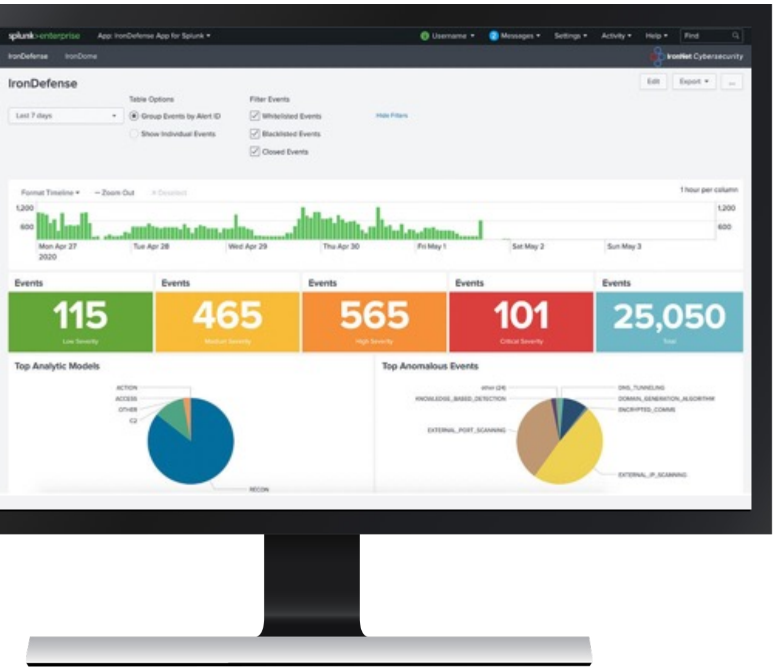
- Target selection is typically done through mass vulnerability scanning, phishing, credential stuffing, buying RDP accesses from underground shops, and Fortinet VPN exploits.
- Once gaining initial access, the threat actors deploy LockBit ransomware, which once executed, will immediately begin trying to enumerate all accessible directories and network shares inside the victim system.
- When completed, the payload encrypts each file with a different random AES key. It also begins exfiltrating critical data, which the attackers upload to a free file upload service to use for extortion while negotiating with the victims. After files are encrypted and backups are deleted, the system wallpaper is replaced with an image stating all files are encrypted and to visit a specific .txt file that provides instructions on steps to restore the files.
- Given that LockBit was most active in May 2021, we should expect to see increased activity from this ransomware family in the future and progressively see this name popping up in the news in coming months.

3 A security ecosystem with strategic technology partner integrations

IronNet Technology Partners

To IronNet, technology integration is not just building a network of best-in-breed partners. Instead, it is about enabling you to build a security ecosystem for faster detection and response. For example, IronNet's technology partnership with leading endpoint protection provider CrowdStrike allows organizations to apply the unique capabilities of both platforms together to see more broadly across the cyber threat landscape — and more effectively defend against cyber attacks.





IronDefense

Last 7 days

Table Options: ● Group Events by Alert ID ○ Show Individual Events

Filter Events: ☑ Whitelisted Events ☑ Blacklisted Events ☑ Closed Events

Events	Events	Events	Events	Events
115	465	565	101	25,050
Low Severity	Medium Severity	High Severity	Critical Severity	Total

Top Analytic Models

Top Anomalous Events

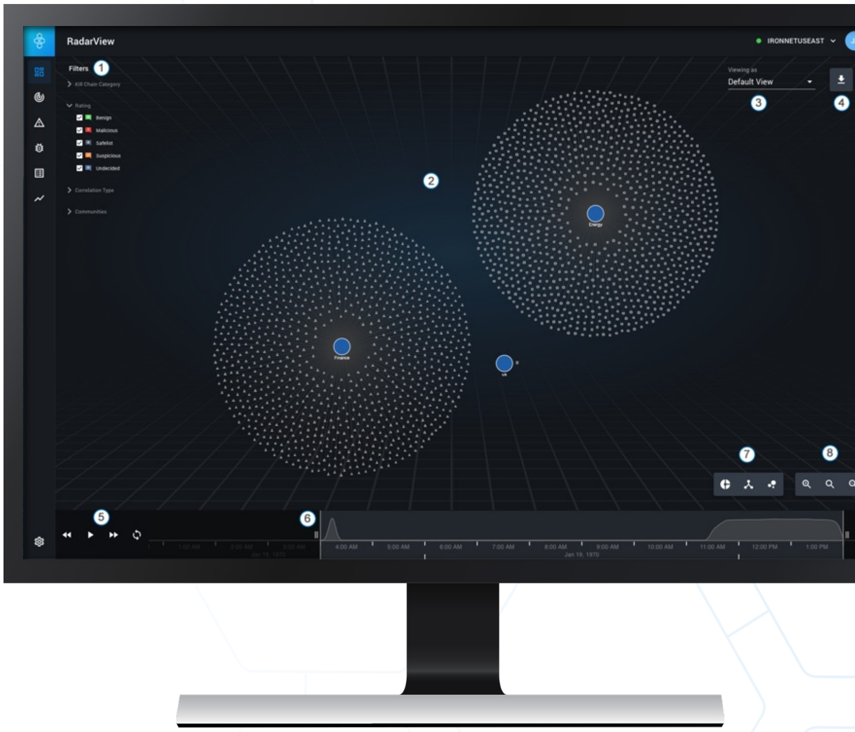
IronDefense Splunk integration

IronNet integrations in Splunk and QRadar receive all detection information in a format that is conducive for additional correlation within the SIEM. In addition, SOAR integrations in Phantom, XSOAR (formerly known as Demisto), and Swimlane expose the same endpoints for ingesting detections and responding with analyst feedback. The SOAR integrations also expose the ability to send IoCs from threats detected on the enterprise to IronDome to determine if the threat had been seen previously by other anonymized customers of IronNet and to provide the ability to distribute signatures (threat intelligence rules). This capability allows all IronDome participants to benefit from the shared (anonymized) intelligence derived from the detected threat.

4

A Collective Defense platform for real-time threat correlation across multiple organizations

IronNet builds secure Collective Defense communities in which organizations from a sector, supply chain, or country can share threat data anonymously to provide all members an early warning system about potential incoming cyber attacks, including the early network intrusion activity associated with ransomware attacks. IronDome's cyber RadarView dashboard gives enterprises dynamic, real-time visibility of the threat landscape in order to respond faster to correlated threats.



IronDome RadarView dashboard

IronNet™

Act now against ransomware attacks

Connect with us to learn more about detecting ransomware early with NDR