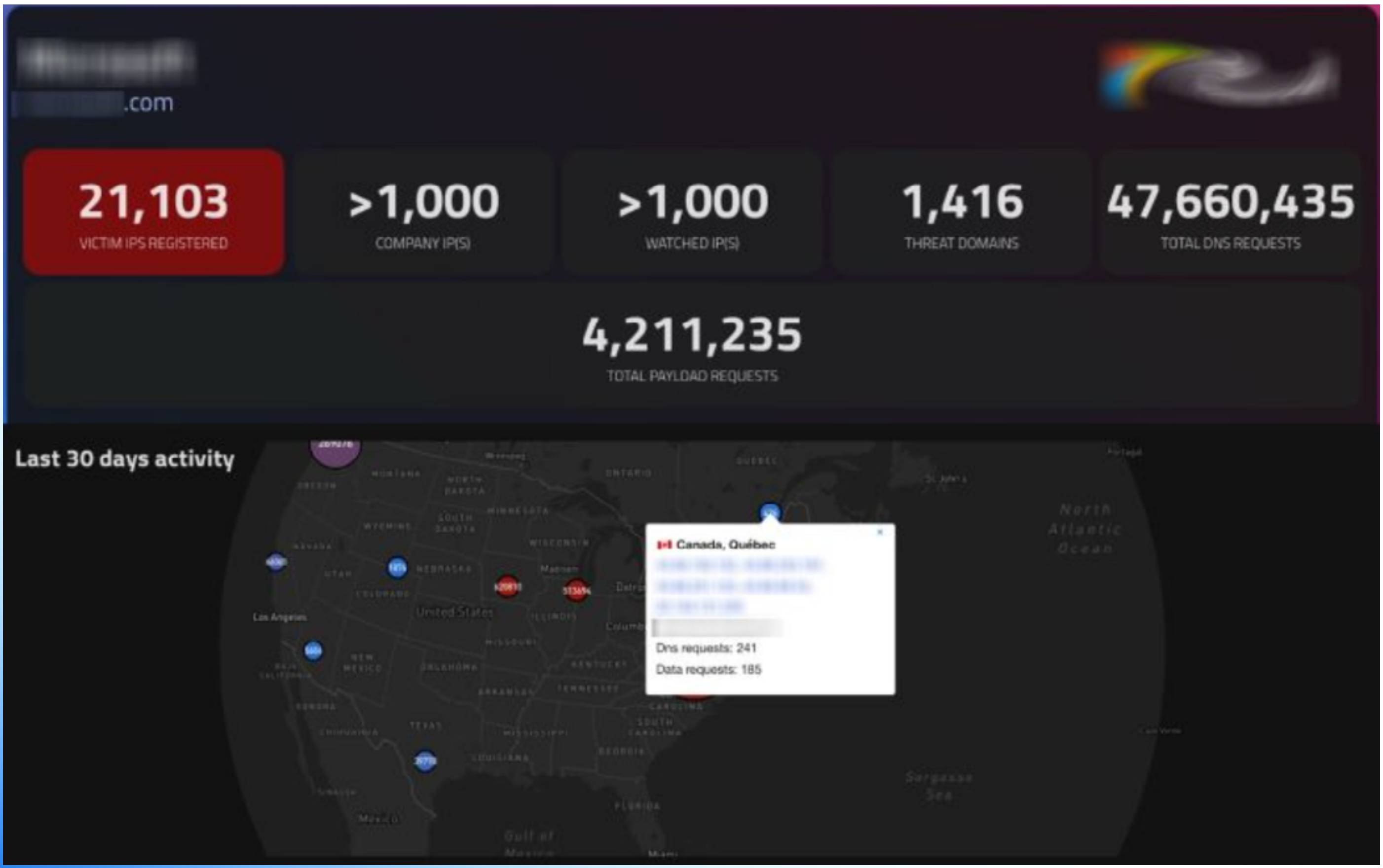
V-Detect is a unique Evidence of Compromise (EoC) breach intelligence platform, it goes beyond conventional approaches to provide materiality of breach intelligence. It has the ability to identify and interdict (see glossary) C2 domains, perform a 3 way handshake with the malware, becoming the receiver of the malware. Without detection from the adversaries.

These are confirmed security breaches, real data, that has negated all other security controls.

There is also a vast data lake of pre-weaponised infrastructure, this provides pre-emptive security – We are the only company who has the ability to derive this data, making the capability unique to us and our partners.



[redacted]

[redacted].com

21,103
VICTIM IPS REGISTERED

>1,000
COMPANY IP(S)

>1,000
WATCHED IP(S)

1,416
THREAT DOMAINS

47,660,435
TOTAL DNS REQUESTS

4,211,235
TOTAL PAYLOAD REQUESTS

Last 30 days activity

Canada, Québec
[redacted]
Dns requests: 241
Data requests: 185

The process: Available under NDA

[redacted]

The above is a walkthrough on the platform and the journey, but the platform is almost entirely automated, the parts where our analysts make decisions is mainly over what we chose to interdict. This could range from the most interesting campaigns, due to known actors, size and scale, uniqueness, proliferation etc. etc. Or a specific request from LE, Intelligence Agency, or a customer-specific request.

From there we agree with the customer on the workflow, automated alerts, reports will be delivered to a 3rd party secure messaging platform with MFA and not via email. Frequency, review, overtime statistics, industry/competitor comparison etc. is all possible but requires discussion and possible development should the requests be non-standard.

There three main phases in the Venari V–Detect process

1 – Determination of maliciousness of inbound domains.

Determining the maliciousness of newly registered domains at large scale involves a combination of orthogonal automated and manual processes, specialised tools, and human expertise to understand the characteristics, behaviour, and potential impact of threat actors and campaigns.

A summary of the key components involved in this process at scale:

Sandboxing and Malware Detonation, Static Analysis, Memory Analysis, Reverse Engineering / Code Disassembly, Network Traffic Analysis, Data and Artifact Analysis, proprietary Intel creation and integration, OSINT integration, machine learning and deep learning model development and integration, understanding TTPs to aid attribution.

2 – Automated issuance of Domain delegation

Once a domain is interrogated and found to be a valid candidate for domain suspension, there is an automated process - with threat analyst oversight - to ensure this domain is delegated from the domain registrars. The threat analyst oversight is an essential phase, we must be sure that our true positive ratio is accurate.

3 – Interdicting traffic from specific threat campaigns

Once a domain is delegated, we automatically spin up appropriate infrastructure as part of the SaaS service to act as an endpoint for compromised hosts. We can then use this to understand the role of the domain in the attack lifecycle (from initial phish to data exfiltration). This vector of the attack is now interdicted and acts as a beacon for that specific campaign.

Note, at the point of domain interrogation there is a limited understanding of the scale required once the domain is delegated. Botnets or victim networks can range from a few infected hosts to many millions, depending on the nature of the campaign. There is significant cost to Venari in the spin up of appropriate infrastructure to cater to this potential scale and the requirement for TLS termination from compromised or breached endpoints - including the automated creation of Certificate chains.

To summarize, there are many challenges and problems associated with traditional Threat Intelligence and IoCs including false positive rate, over-reliance on IoCs, IoC staleness, attribution challenges, implementation, and integration costs.

We believe that our ability to provide "Evidence of Compromise" offers a market first, significant, and tangible value with game changing benefits over the traditional approach.

For a customer this is zero touch technology, all that is needed is a customer public CIDR.

Middleware test and discovery:

Venari recognizes that systems which are only triggered when a serious and material breach occurs can be hard to test. We understand that you do not want to connect 'known bad' for the purposes of testing.

Venari provides a Middleware component to which you can connect from any of your registered sites which, with no risk to your infrastructure:

Records your session and host information in detail

Establishes an outbound connection to known bad with your details recorded in the packet headers (standard X-Forwarded-For)

Responds to you test connection with the session summary

This test data will be reflected in the Portal.

Glossary

C2 traffic

C2 traffic refers to Command and Control traffic in the context of cybersecurity and malware. It involves communications between compromised devices (such as computers or servers) and an external controller operated by an attacker. The controller, often referred to as a Command and Control server or C2 server, is used by cybercriminals to remotely manage and control compromised devices.

C2 traffic typically includes commands sent from the attacker to the compromised devices, instructing them to carry out malicious activities such as executing commands, downloading and installing additional malware, exfiltrating data, or participating in coordinated attacks (such as distributed denial-of-service attacks).

Detecting and blocking C2 traffic is critical for defending against cyber threats, as it can help prevent attackers from maintaining control over compromised devices and carrying out further malicious actions.

Interdicted domain

This is any domain “seized” or interdicted by V-Detect malware command and control interdiction framework. Typically, malware campaigns use many, many domains during the attack lifecycle. Interdicted domains represent a small sample of this real list of domains used by a malware campaign. Activity to any interdicted domain is an indicator of the success of a specific malware campaign and the failure of a victim’s security defences.

Public IP Egress Count & IP Address Count

The total number of unique Public IP Addresses that communicated with the Venari Security infrastructure during the reporting timeframe. Due to the nature of modern networking (NAT, CGNAT et al) each Public IP address seen here might represent only one or many hundreds of private, compromised or victim systems.

DNS Queries

The total number of domain requests for Interdicted domains. Activity here shows that the malicious campaign is active and compromised end-user machines or servers are attempting to reach the command and control (C2) infrastructure of the malware campaign to either exfiltrate data or receive instructions.

Payload Queries

The total number of successful requests for Interdicted domains. Activity here shows that the malicious campaign is active and compromised end-user machines or servers are successfully reaching the command and control (C2) infrastructure of the malware campaign to either exfiltrate data or receive instructions.

Please Note: Both DNS queries and Payload queries represent activity by breached or compromised hosts. In the case of Payload, this activity is successfully and freely bypassing all existing security controls within the victim’s network and reaching its intended target for either data theft or to receive further instructions from the threat actor.

Fast flux DNS

DNS fast fluxing is a technique used by malicious actors that involves associating multiple IP addresses with a single domain name and changing out these IP addresses rapidly. Sometimes, hundreds or even thousands of IP addresses are used. Attackers use DNS fast fluxing to keep their web properties up and running, hide the true origin of their malicious activity, and stop security teams from blocking their IP address.

Attackers need their websites to stay up in order to carry out phishing attacks, host malware, sell stolen credit card information, and perform other illegal activities. With DNS fast flux, malicious domains have more uptime and are harder to block, enabling cyber criminals to carry out more attacks. Essentially, DNS fast fluxing turns malicious domains into a moving target.

Bridge your knowledge gap.
Visit: www.venarisecurity.com

Venari Security Ltd.
16 Great Queen Street, London,
WC2B 5AH, United Kingdom
+44 (0)20 7294 7749
info@venarisecurity.com

About Venari Security

Venari Security provides organisations with advanced visibility into their encrypted attack surface, ensuring regulatory compliance and privacy adherence through our cryptographic discovery tool.

Our focus is on crypto agility which helps you assess both external and internal cryptographic risks, preparing your business now and for the quantum future.