



USE CASE

Passive DNS: The Context of IP Addresses

When threat actors target financial institutions using ransomware, they deploy it via multiple IP addresses. (If they use a single IP address, cybersecurity monitors pick it up too easily.)

Workstations infected by ransomware communicate with attackers' command and control infrastructure (also called C&C and C2), which is a requirement for conducting a successful cyber attack. Cybersecurity professionals rely on this telemetry – data obtained from networks and analyzed for monitoring network security – which typically confirms what IP addresses the threat actors are likely to use in the attack as part of their C2.

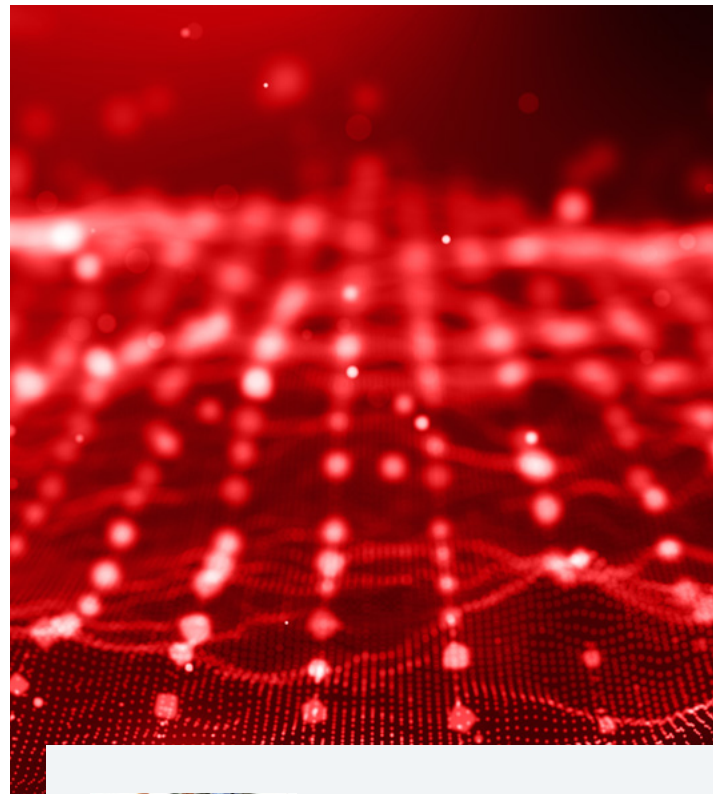
To prevent cyber attacks wreaking havoc and causing fallout for organizations, cybersecurity professionals monitor the domain name system (DNS), which is increasingly used by cyber criminals for these nefarious ends.

Passive DNS – automatic, continuous monitoring of potential threats – is (and should be) a feature of complete DNS protection solutions.

Most people don't tend to read or type IP addresses like they do domain names. IP addresses are domain names that have been translated so computers communicating with each other can read and understand them.

This process of translation is known as resolution: DNS resolves to IPs. As such, if you can identify domain names used by attackers, then pivot to their (domain name) registration details, you're able to gain valuable C2 data in helping thwart attacks.

Using passive DNS is an essential tool for tracking bad actors. Searches on particular IP addresses reveal the locations around the world as the sources of those addresses, but passive DNS shows the domain names that have resolved to the specific address. This provides context for IP addresses so that cybersecurity professionals can see how threat actors are using their C2.



DAVID BRUNSDON, Threat Intelligence Security Engineer at HYAS outlines a popular attack vector targeting major financial sector institutions every day and details how HYAS solutions identifies and stops it.

“Passive DNS – automatic, continuous monitoring of potential threats – is (and should be) a feature of complete DNS protection solutions.”

Passive DNS tools can also provide information about C2 attribution: Other cybersecurity teams provide data that identifies C2 infrastructure, which then alerts all teams looking at a particular likely threat actor that there is definitive nefarious activity going on. It also provides threat intelligence teams with bad actor IP addresses to pivot off from C2 domains used by these actors.

HYAS Insight Into Every Use Case

Threat and fraud researchers and investigators in the financial industry can easily build up dossiers of attacks to take to and promptly notify relevant law enforcement agencies. We have unique data. And being able to pivot from one data point to another data point, especially when we've got unique data, becomes extremely valuable.

HYAS Insight offers threat intelligence, data point pivoting and unique data capabilities invaluable for financial organizations who want to stop the myriad cyber threats that they face. The ability to uncover domain registrations not available to most other cybersecurity solution providers delivers the whole financial sector with the confidence to conduct business operations in the face of malware attacks and phishing campaigns.

Pivoting from single suspicious domains and IP addresses can ultimately uncover vast campaigns designed to destabilize business purely for financial gain. But organizations armed with relevant, unparalleled insight can ensure that bad actors don't get far.

Additional Resources

[Case Study: HYAS Insight Shines a Light on Financial Fraud](#)

[How HYAS Protects the Financial Services Industry](#)
[HYAS Insight Threat Intelligence and Investigation](#)
[HYAS Protect Protective DNS](#)

Banking on the Right Protection

- The financial sector is a prime target for cyber attacks. Financial organizations and their customers and clients feel the fallout of major ransomware and phishing campaigns more than ever, and there's often more at stake.
- Finance needs a new approach to deal with the ongoing rise in cybercrime. The right tools coupled with unique data function as preventative measures against threat actors using innovative methods to target and exploit organizations and individuals alike.
- Even the most sophisticated ransomware attacks and phishing campaigns are not invulnerable. Leveraging advanced cyber threat intelligence and investigative tools powered with the right data can stop those responsible for cybercrime in the financial sector a lot more easily.

CONTACT US

hyas.com/contact

INVESTIGATE ATTACK
INFRASTRUCTURE FURTHER
AND IDENTIFY FRAUD FASTER



HYAS INSIGHT

An efficient and expedient investigation is the best way to protect your enterprise. HYAS Insight provides threat and fraud response teams with unparalleled visibility into everything you need to know about the attack. This includes the origin, current infrastructure being used and any infrastructure.



PROTECTING BUSINESSES AND SOLVING INTELLIGENCE PROBLEMS
THROUGH DETECTION OF ADVERSARY INFRASTRUCTURE AND
ANOMALOUS COMMUNICATION PATTERNS

HYAS is a world-leading authority on cyber adversary infrastructure and communication to that infrastructure. HYAS is dedicated to protecting organizations and solving intelligence problems through detection of adversary infrastructure and anomalous communication patterns.

We help businesses see more, do more, and understand more in real time about the nature of the threats they face. HYAS turns meta-data into actionable threat intelligence, actual adversary visibility, and protective DNS that renders malware inoperable.