3 Cyber Threats MSSPs Can Help Their Clients with Using Reverse NS API

Posted on December 9, 2019

```
    mirror_mod.use_x = False
    mirror_mod.use_y = True
    mirror_mod.use_z = False
elif _operation == "MIRROR_Z":
    mirror_mod.use_x = False
    mirror_mod.use_y = False
    mirror_mod.use_z = True

    #selection at the end -add back the deselected mirror modifier object
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.objects.active = modifier_ob
print("Selected" + str(modifier_ob)) # modifier ob is the active ob
    #mirror_ob.select = 0
```

Did you know that the cybercrime economy may currently well be worth US $1.5 trillion? According to figures from an independent study, that's how much professional crime networks worldwide earned in 2018.

That amount is just a little over 1% of the world's gross domestic product (GDP). It is also comparable to the GDP of a country like Russia.

Other cybercrime revenue estimates reveal:

- Revenues from intellectual property or trade secret theft amounted to US $500 billion.
- 2014 estimates reveal that the global cybercrime revenue reached US $600 billion.
- Security events cost small businesses an average of US $200,000 per incident. Most victims close up shop within six months of each incident.

These statistics reflect the scale of losses businesses incur due to cyber attacks. And with many organizations incapable of battling such threats, most have transferred the herculean task to managed security service providers (MSSPs).

MSSPs offer companies round-the-clock protection against attacks, provided they have the right threat-hunting toolsets. A reverse NS API provides MSSPs accurate domain intelligence that can enrich their incident data and bolster security layers against future risks.

Here are ways by which Reverse NS API can help MSSPs obtain real-time situational awareness to mitigate today's most notorious attack types.

Distributed Denial-of-Service (DDoS) Attacks

DDoS attacks occur when thousands of bots overwhelm a server by flooding it with bad or useless traffic. These could happen to the best of companies — even Amazon Web Services (AWS). While the tech giant downplayed news of the attack, several tech sites revealed that it lasted for about eight hours, putting several AWS-hosted sites offline. Here’s what we know so far:

- The attack targeted Amazon’s Simple Storage Service (S3). Several domains were affected.
- Shield Advanced, Amazon’s own DDoS mitigation service, flagged a great deal of the trash Domain Name System (DNS) traffic, as well as legitimate queries.
- Amazon and a third-party DDoS mitigation service provider that it works with initiated incident response five hours into the attack.

Solution

Understanding the warning signs of application-layer attacks is the first step toward mitigation. Fake DNS traffic may fall below the baseline. In some cases, attackers merge bad traffic with equal volumes of real user traffic to evade detection. Thus, being hyper-vigilant of unusual DNS requests can help thwart attacks in time.

Integrating a reverse NS API into an intrusion prevention system (IPS) allows users to identify hijacked domains practically in real time. The tool enables users to check for web server overload, which may disrupt their business. It also allows them to uncover compromised domains or nameservers.

Insider Threats

No company is immune to insider threats. All it takes is one employee obtaining a private key to create soft tokens or altering their boss’s credentials to compromise an entire database’s security.

However, in many cases insider threats are not even intentional. Spearphishing and data leakage often result from human error — mishandled credentials, clicking on phishing links, or misdirecting emails.

No matter the case, though, insider threats have far-reaching consequences. For instance, in 2016, the average cost of a spearphishing attack was said to be worth US $1.8 million in the U.S. Meanwhile, insider threats cost companies between US $489,100 and US $26.5 million.

Solution

Perimeter security has no use in the event of insider attacks. MSSPs need a program that provides them with deep visibility into their networks before threat actors can steal information.

Hackers can use backdoors to exfiltrate data over DNS from infected hosts easily. Accurate reverse NS lookups can expose system misconfigurations and malicious nameservers that may be communicating with their users' networks.

Analysts can cross-reference mail exchange (MX) records with Reverse NS API to gain insights into data movements and user behaviors. They can also incorporate it into their intrusion control systems to identify other forms of DNS anomalies or just use it for data enrichment for penetration testing.

Ransomware Attacks

Ransomware incidents have been all over the news sites lately, as new variants targeted public and private organizations. Some variants can also affect critical infrastructure and cause massive disruptions. In 2017 alone, businesses lost US $5 billion due to ransomware attacks.

Recent ransomware attack victims include Billtrust, a B2B payments managing platform; Italian residents, who received spam from fake tax revenue service employees; and a New Mexico public school.

Solution

Applying the “least privilege” principle can make a massive difference in spotting deviations in log records. The use of robust antispam and antiphishing technologies, such as data loss prevention (DLP) software and Reverse NS API, allows security providers to prevent phishing emails from making it to users’ inboxes.

Reliable data from the API can also supplement threat intelligence for cyberforensics and penetration tests. Infosec professionals can also use correct nameserver data to refine rule-based controls for email and firewall filters.

Cyberthreats may grow further in sophistication, but companies don’t have to remain vulnerable. Tools like Reverse NS API can aid MSSPs’ threat-hunting and mitigation efforts by providing actionable threat intelligence.