Attacks Are Tailored to You—Your Intelligence Should Be, Too.

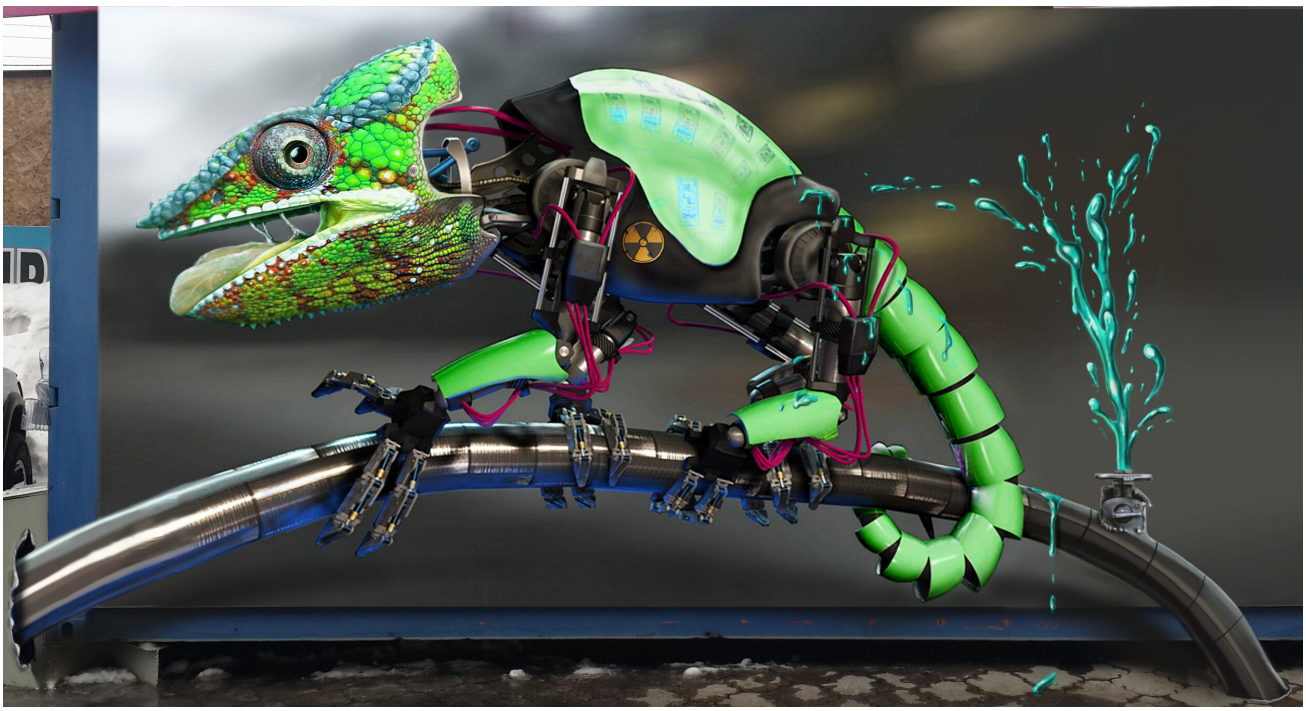
silentpush.com/blog/targeted-attacks-and-generic-defense-dont-match

July 16, 2021

Jul 16

Written By Ken Bagnall

2021 may well be called, “the year of the targeted attack.” Over and over, threat actors have carried out carefully crafted operations using infrastructure tailored to specific victim organizations.



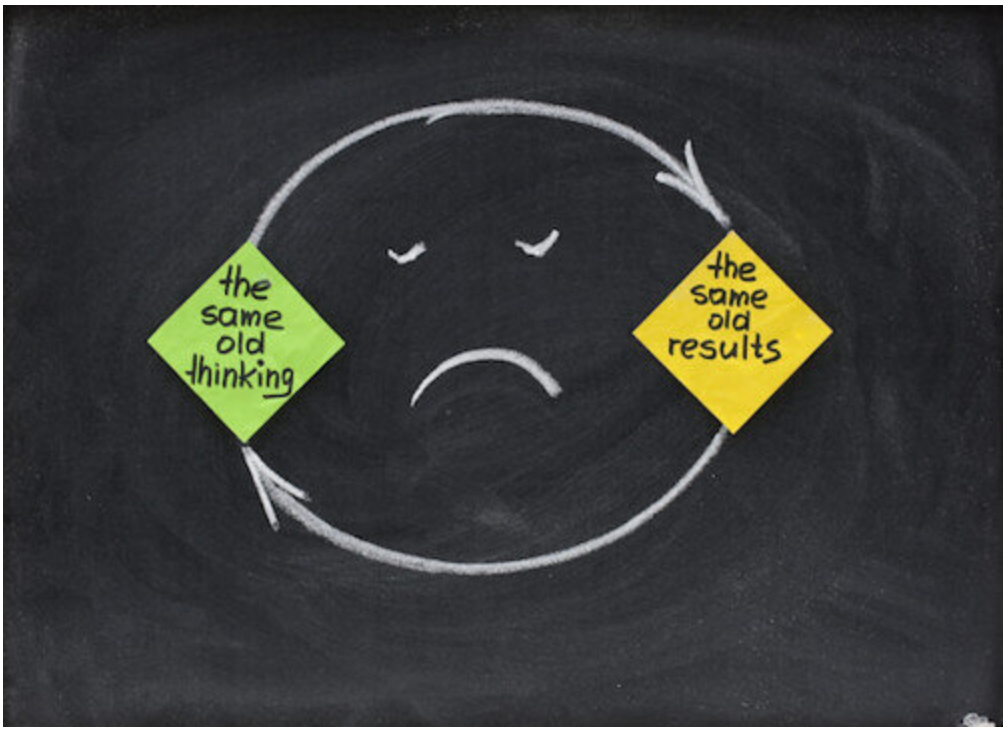
On the other side of the table, large organizations rely on security tools that, at best, attempt to block the indicators they observed hitting other organizations previously. These IOCs don’t necessarily relate to the defending organization, meaning blue teams regularly miss the actors crafting domains and infrastructure to get beyond their particular defenses.

It is too easy for the organized crime or espionage group to develop new, bespoke assets to attack an organization safe in the knowledge of how to evade traditional security products and services. We regularly see assets set up with such specific evasion techniques in mind.

We see domains registered and then aged for a period of time before malicious use to avoid aged based reputation scores; we see domains imitating supply chain partners of various types to avoid security practitioners and potential victims becoming suspicious

when seeing them in logs*;* we see rotating name servers and customized name servers in order to communicate with specialized malware while avoiding fingerprinting rules and behavior-based detection techniques. At the same time, we see very few innovations from security vendors to react to these new techniques. It's time for the security industry and those defending teams to fight back.

We want to equip enterprises with the freedom to protect themselves.



Everybody needs their own customized threat intelligence. If an organization can't meaningfully search for the attacks that are being tailored to them, what chance do they have?

We are exposing the analytics to help organizations track and trace the very attacker infrastructure being designed just for them. We allow threat intelligence teams to shine a light on this infrastructure as it is going live so they have a chance to *proactively* defend their organizations instead of hoping to discover the infrastructure after it's hit someone else.

Enterprises have been expected to accept 'black box' thinking from their security vendors for years: 'You don't need to know the details of how we detect things, just pay us the money and trust that we are defending you.' That clearly hasn't worked.

We are now exposing the underlying connections and patterns to enable enterprises to create *their own* intelligence feeds, focused on what *they* need to defend against.

If 5 threat groups use the same malicious infrastructure provider, then the enterprise needs to defend against that infrastructure provider. If numerous advanced threat groups use the same technique of managing and aging domains over time, then the enterprise needs to be able to identify domains currently managed with that technique going live. If a virtual Bullet Proof Hosting Provider is the commonality across numerous campaigns by different groups then a defending enterprise must be able to identify the fingerprint of that provider to defend against it.

These are the things we can allow the enterprise to do. We want to empower enterprise Threat Intelligence teams with the tools to generate their own new intelligence and to fuse their current intelligence with new insights that help contextualize and prioritize what matters today.

Subscribe

Sign up with your email address to receive news and updates.

We respect your privacy.

Thank you!

Ken Bagnall