Domain Monitoring Service

Challenge

Defenders face numerous challenges trying to protect organizations from cyber attacks. Many of the tools available take a reactive approach to threats, leaving organizations to wait for attacks and hope that their defenses will detect or stop them. Monitoring domain registrations is one way to proactively detect when criminals stand up infrastructure to be used in a future attack.

Attackers frequently attempt to bypass existing security controls by registering domains that mimic authentic corporate infrastructure. These domains can be weaponized within hours of registration and subsequently used for delivery of malicious payloads and exfiltration of sensitive data. The ability to detect these malicious domains within one hour of registration is therefore essential to a proactive security posture.

The Anomali Domain Monitoring Service is a yearly subscription that includes monitoring a customized number of domains or keywords for new suspicious registrations. This service enables security teams to:

- Detect attacker infrastructure before it is used;
- Disrupt an attacker's ability to create an outbound channel (e.g command and control);
- Prevent harvesting and exfiltration of data.

How It Works

The Anomali proprietary algorithm identifies homoglyphs — characters that appears very much like another (e.g. number 0 and uppercase O) — and look-alike domains and converts them to IOCs in ThreatStream within one to four hours of generic top-level domain (gTLD) registration. Seasoned security analysts and threat researchers also manually review and report (within 48 hours) any additional anomalous activity associated with registrations.

Identified domains are imported into ThreatStream and customer integrations, automatically providing clients with:

- Alerts of newly registered domains;
- Details of newly registered domains as Threat Bulletins;
- New potential Indicators of Compromise (IOCs) for further investigation.

The Domain Monitoring Service also detects and reviews domains that may be in violation of corporate brand infringement.

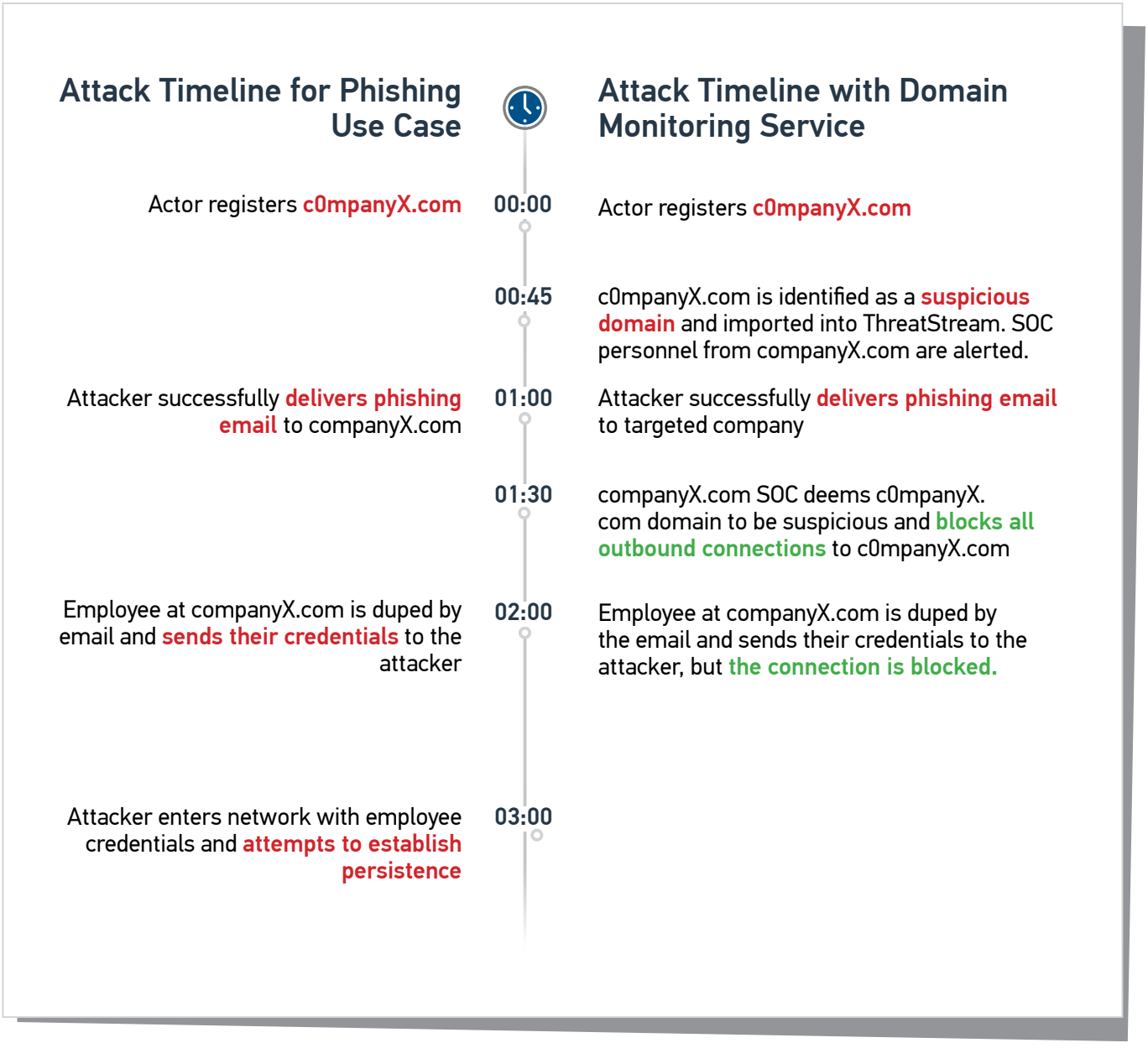
Use Cases

Homoglpyhic and look-alike domains play an integral role in various parts of the Cyber Kill Chain. For the example of companyX.com, a malicious actor may register the domain c0mpanyX.com. This domain can then be weaponized and subsequently used in one to all of the following common attack vectors:

1. **Phishing attack** (Delivery part of the Kill Chain). An email is sent to an employee attempting to entice them to send their credentials to dropbox.c0mpanyX.com.
2. **Command and Control** (Command and Control part of the Kill Chain). Attacker configures their backdoor or malware to communicate to c0mpanyX.com for further instructions.
3. **Exfiltration** ("Actions on Objective" part of the Kill Chain). Attacker sends stolen data back to c0mpanyX.com. This homoglyphic domain may be

missed by companyX.com's security team.

The following attack timelines outline the sequence of events for a Phishing attack with and without the Domain Monitoring Service. In both cases, the attacker is successful in tricking an employee to reveal their credentials. The idea being that, even with a very effective phishing awareness program, given enough phishing attempts — some will be delivered and eventually someone will click. With the Domain Monitoring Service, companyX.com is able to intervene and prevent any critical damage.



For additional information or to schedule a consultation please contact
cso-ps@anomali.com

Corporate office: 808 Winslow Street, Redwood City, CA 94063

ANOMALI®