



From Trust to Threat: How attackers Leverage Trust to Breach Systems

Ali Haidar Chief Customer Advocate



ANOMALI

Introduction



Humans: The Weakest Link in Cyber Defense

Targeting the Human Element: A Growing Trend

Threat actors understand that humans are the weakest link in an organization's cyber defense

With traditional technical defenses becoming stronger, threat actors are leveraging new techniques to target and manipulate human behavior

In the following slides, we will explore the most common methods recently used by threat actors and provide recommendations to combat this rising threat.





Rise of Adversary Adaptation

Current Focus of Cyber Defense

As cybersecurity advances, most of an organization's defense technology is concentrated on protecting entry points to an organization, such as the email system or web system.“

Significant investments have been made in research and resources for systems like:

- Email Security Systems
- Firewalls
- Intrusion Prevention Systems (IPS)
- Web Filtering

Attackers now seek to bypass traditional defenses by leveraging user trust and manipulating human behavior.



From Phishing to Social Engineering: The New Approach

New Techniques Gaining Popularity

Since the infamous Geek Squad phishing campaign, more threat actors are adopting these new techniques to compromise individuals and organizations

The latest trend is to send a socially engineered email with no malicious attachments or links. Instead, attackers include a contact phone number or a web chat link.

If the user engages, the threat actor then convinces them to install malicious software on their own device. Attackers now seek to bypass traditional defenses by leveraging user trust and manipulating human behavior.



Targeting Employees Beyond the Perimeter: Social Media Exploitation

Rise of Social Media Attacks

With the rise of social media and remote work, threat actors are increasingly targeting company employees through social media platforms.

The strategy is to gain the employee's trust and lure them into executing malicious content on their remote work equipment.

North Korea has been particularly successful in using this method, as demonstrated by the 'Dream Job' campaign.

This campaign involved creating fake job offers and engaging in conversations with employees to eventually convince them to download malware under the guise of job-related content.



Exploitation of Trusted Systems: The Ultimate Breach

The Deadly 3

The most dangerous exploitation of trust comes from leveraging an already trusted and authenticated system.

The SolarWinds breach was a perfect example of a supply chain attack, where threat actors compromised a trusted software update, leading to widespread infiltration.

The North Korean Fake IT Worker campaign involved attackers posing as legitimate employees to infiltrate organizations and exfiltrate sensitive data.

Black Basta has been recently reported to utilize compromised legitimate email accounts of trusted third-party vendors to craft convincing phishing emails to target customers and business partners



Approaches to Detecting Trust Exploitation Attacks

Behavior Or Alerting?

Detecting trust-based attacks requires a combination of advanced techniques due to their subtle and deceptive nature

Behavioural Analytics:

- Leverages Machine Learning and User and Entity Behavior Analytics (UEBA) to identify anomalies and suspicious patterns that deviate from normal user behavior.
- Challenges: High potential for false positives without proper tuning and requires a mature data model for accuracy

MITRE Alert Mapping:

- Maps detected events to known adversary tactics and techniques based on the MITRE ATT&CK framework.
- Challenges: Requires high-fidelity data sources and may miss novel tactics not yet documented in the framework.

Recommended Strategy

The optimal approach is a **merged strategy** that integrates both methods, providing detection-in-depth for comprehensive coverage and higher accuracy.



“Q&A”

Thank You
Contact Email:
ahaidar@anomaly.com