

How Zscaler[™] Can Disrupt the Cyber Kill Chain

An Infrastructure Security Review by the
Zscaler Solution Architect team

A review of security controls available through the Zscaler service
to detect and prevent cyberattacks

Yogi Chandiramani – yogi@zscaler.com

How Zscaler can disrupt the Cyber Kill Chain

Document Purpose

The purpose of this document is to explain how Zscaler can protect organisations against Advanced Persistent Threats (APTs). It will describe in depth how attackers typically compromise organisations and exfiltrate information. The foundation of the discussion will be the cyber kill chain model, and how attacks can be prevented by disrupting the cyber kill chain. This discussion will enable the reader to understand how to detect and prevent APTs and deliver a secure and robust security service.

THE CYBER KILL CHAIN MODEL

The threat landscape has evolved over the years and threat actors are constantly changing their Techniques, Tools, and Procedures (TTPs) to compromise organisations. TTPs encompass:

- **Techniques:** The method used to compromise the victim's workstation
- **Tools:** The type of malware used to compromise the victim's workstation
- **Procedures:** How the data is collected and exfiltrated once a workstation is compromised

Once a workstation is compromised, it is controlled by the threat actor, whose objectives are generally one of the following:

- **Financial gain:** Ransomware payment, for example
- **Intellectual property:** Cyber-espionage
- **National security information:** Intel gathering
- **Destruction:** Cyber-sabotage

The potential gains from attacks — and practical impunity with which they're carried out — make it attractive for threat actors to continue to develop and execute new attacks. Even though attribution has been associated with a few attacks that were made public, consequences for threat actors are extremely limited.

THE CYBER KILL CHAIN MODEL CONSISTS OF SEVEN STAGES:



Figure 1 – Cyber kill chain model

Threat actors execute these stages in sequence to complete their attacks. However, disrupting just one stage of the cyber kill chain can stop the attack entirely. The earlier the chain is disrupted, the less damage it will cause. We'll discuss in the following sections how Zscaler can help disrupt each stage of the cyber kill chain.

STAGE 1: RECONNAISSANCE

During the reconnaissance stage, the threat actor performs research on the target. This research can be done in multiple ways:

- Viewing public websites
- Following employees on social media
- Collecting and scanning technical information such as public IP addresses and potentially vulnerable public servers

LinkedIn and other social media websites make it easy for threat actors to gather intelligence on their potential victims. Typically, threat actors target system administrators, as they have higher system privileges within their organisations. The following screenshots show how database administrators within large enterprises can be found using LinkedIn:

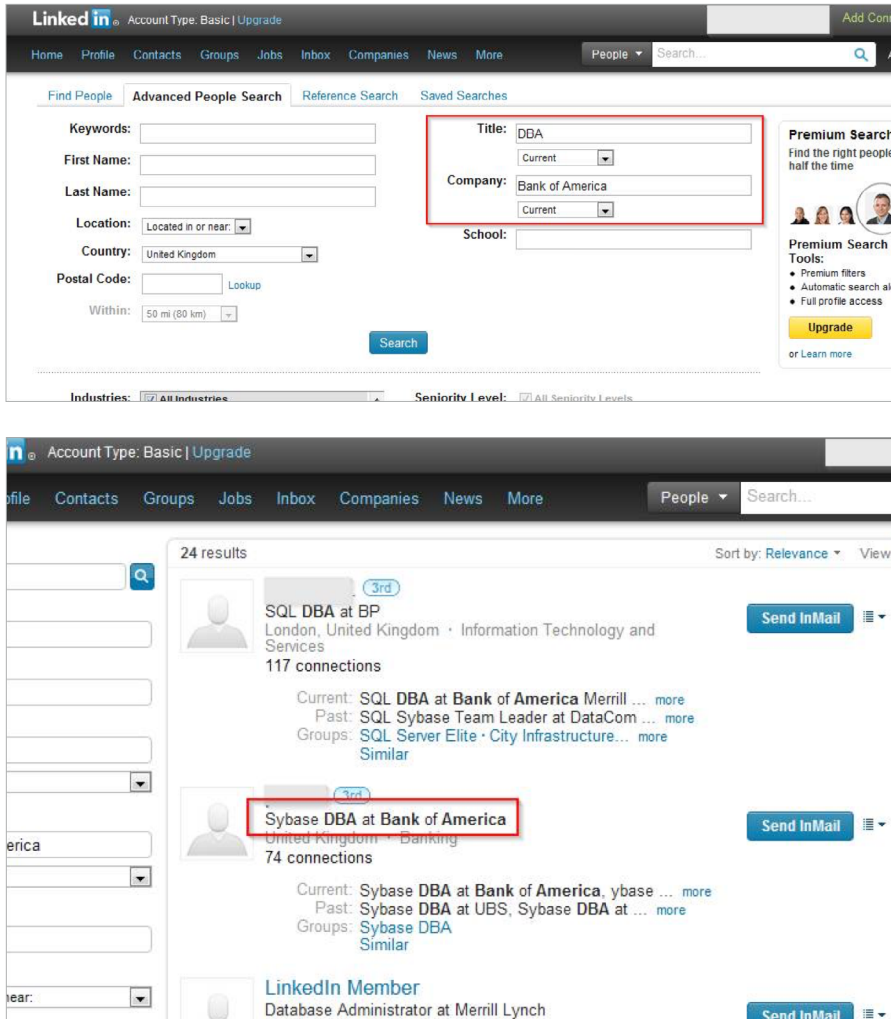


Figure 2 – Searching on social media for database administrators

Additionally, threat actors can try to scan technical information such as IP addresses. All Zscaler customers use Zscaler public IP addresses to connect to websites, and since all their web traffic is forwarded to Zscaler, they are protected against water hole attacks because there is no way for threat actors to serve different content based on their source IP addresses.

Reconnaissance

CYBER KILL CHAIN ATTACK STAGE	KILL STEPS
Social media/Social networking search	It is difficult to create a kill step for this type of action
IP fingerprinting and scanning	Zscaler kills this step by shielding IP addresses in the Zscaler cloud

STAGE 2: WEAPONISATION

Once the target has been identified, threat actors start to develop their attacks by building malicious exploit codes. Exploit codes leverage vulnerabilities, known or unknown, that exist within operating systems or applications. If a workstation is not patched against such a vulnerability, it is subject to the attack.

Threat actors use various techniques to exploit vulnerabilities. For instance, one that is widely used is the “heap spray” technique, in which arbitrary (shell) code is inserted in memory to make vulnerabilities easier to exploit. Once inserted, the system needs to execute that memory space, after which NOP (no operation) instructions are added, directing the system to the memory space where the arbitrary code is running. The following figure provides a high-level view of how heap spray is used on a workstation.

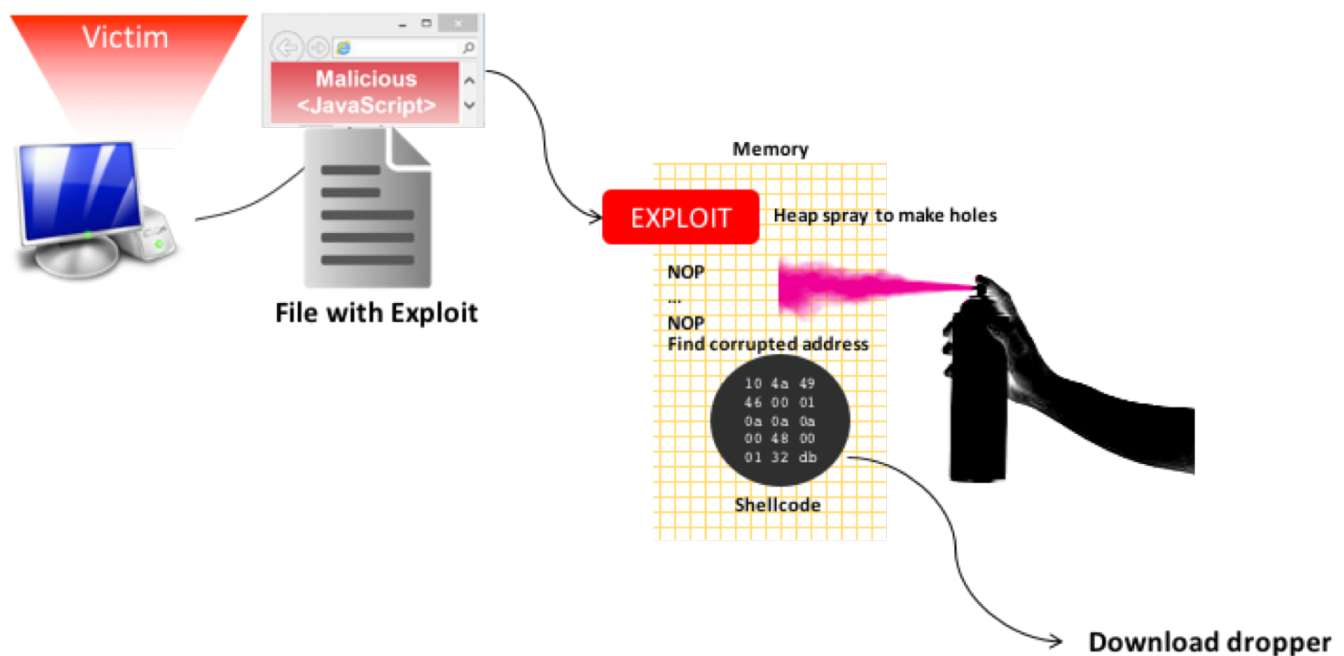


Figure 3 – Heap spray exploit

STAGE 3: DELIVERY

The third step consists of delivering the weaponised document or website with the exploit. Three delivery methods exist:

- Spear phishing
- Web-based attacks (or water holes)
- File-based attacks via email or collaborative tools such as Dropbox, Google Drive, or One Drive

Email is a vector of choice used by threat actors as it allows them to target specific victims. Typically, a threat actor will send a weaponised résumé as an attachment to the HR department. This type of social engineering is effective, as victims often see it as legitimate content. The weaponised document will then attempt to download additional malicious payloads. At this stage, Zscaler security engines inspect traffic and disrupt the cyber kill chain process.

Spear phishing is another APT delivery method used by threat actors. Analysing emails that come in through an SMTP gateway is challenging, as one does not want to click on a one-time link such as password reset links or mailing subscription or simply social media profiles in emails signatures. Furthermore, analysis of spear phishing links is typically performed within a vendor’s cloud, which is often well known to threat actors and malicious content is not delivered when coming from those vendors’ cloud IP addresses. As a result, spear phishing detection is not effective. However, because Zscaler inspects all web traffic, it analyses spear phishing links as soon as a user clicks on them. Let’s now look more closely into how Zscaler provides this protection.

Zscaler intercepts and analyses web traffic, including HTTPS traffic. With SSL inspection, Zscaler customers can inspect file-sharing websites such as Dropbox, Google Drive, and others, even though their traffic is encrypted. Zscaler has implemented multiple layers of inline protections, including:

- Static engines
- Dynamic engines with file detonation in the Zscaler Cloud Sandbox

The following diagram presents a high-level overview of the different engines implemented by Zscaler.

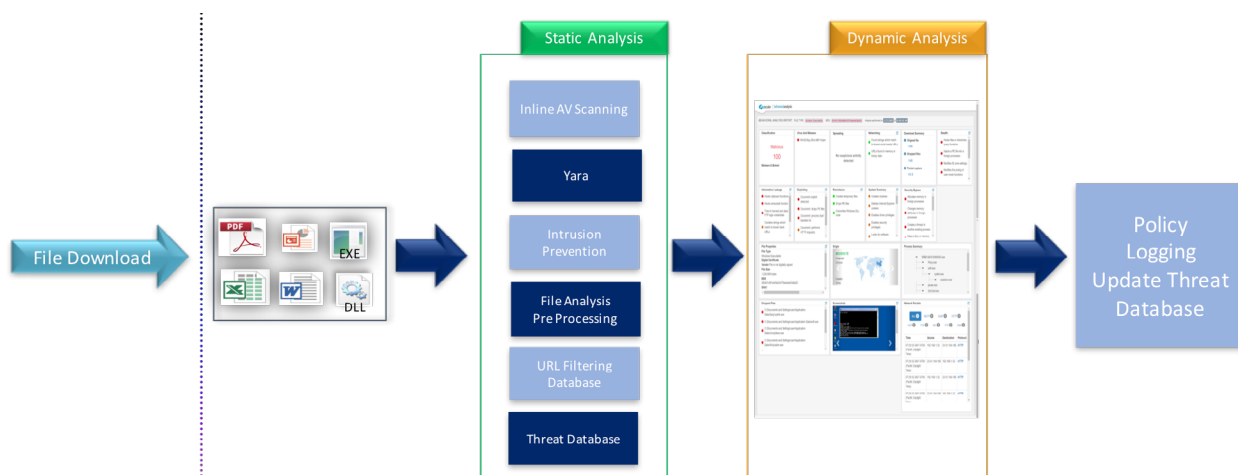


Figure 4 – Zscaler protection engines provide multilayered security

Zscaler is also a member of the Microsoft Active Protections Program (MAPP), through which Zscaler receives advanced notifications of vulnerabilities before they are publicly disclosed. This allows Zscaler to provide earlier, more effective threat protection.

The threat database is a key element of Zscaler protection, as it leverages the “cloud effect.” As soon as a threat is detected within the Zscaler cloud, all users in the cloud are protected within minutes.

Delivery

CYBER KILL CHAIN ATTACK STAGE	KILL STEPS
Email attachment	Zscaler analyses the dropper inline during download
Spear phishing link	Fully protected by Zscaler cloud with inline analysis
Water hole	Fully protected by Zscaler cloud with inline analysis

STAGES 4 AND 5: EXPLOITATION AND INSTALLATION

As in stage 3, the inline static and dynamic inspection engines provide the required protection. As exploits try to evade signature-based protection, the Zscaler Cloud Sandbox effectively analyses the behaviour of the payloads.

Multiple techniques have been designed to evade sandbox analysis. Those techniques are typically grouped within three categories:

- Environmental checks
- Time-based evasion
- User interaction

Environmental checks are used to detect whether an environment is “real” or if it is running on a virtual machine, such as VMware, VirtualBox, or kernel-based virtual machines (KVMs), which would indicate the presence of a sandbox. Zscaler has built the necessary countermeasures to respond appropriately.

Time-based evasion involves the execution of malicious code by waiting out analysis through extended sleep calls. Zscaler analyses behaviour such as “stalling” execution and has built countermeasures to protect against such techniques.

Finally, the user interaction technique requires input from the user, such as clicking a “next” button while some code is installed. Zscaler instrumentation provides input to the sandbox, so it can block the installation of such codes or executables.

This screenshot was taken following detonation in the Zscaler Cloud Sandbox, which prevented the installation of the fake antivirus malware (fakeAV).

Please note that the quarantine feature enables real protection, as files are analysed in the sandbox, avoiding any zero-day patient.

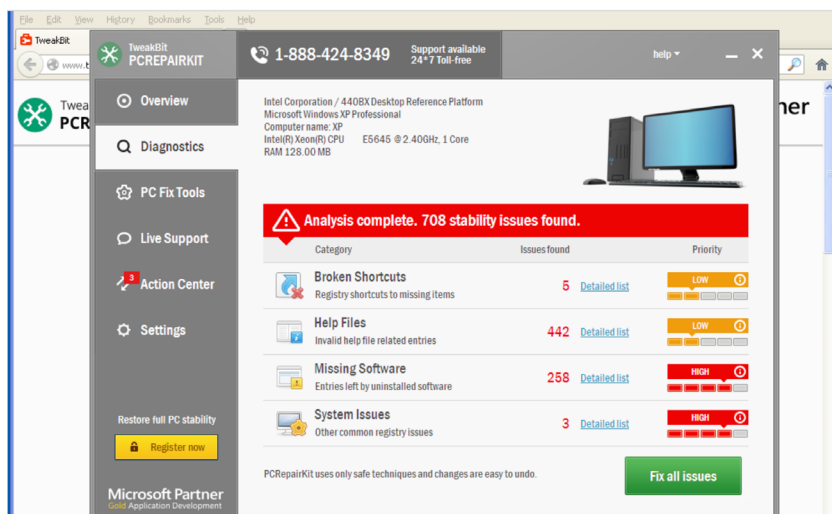


Figure 5 – User interaction instrumentation example

Zscaler offers malicious behaviour detection for Android devices, enabling the identification of any backdoor malware that would be installed on phones and tablets.

Exploitation and Installation

CYBER KILL CHAIN ATTACK STAGE	KILL STEPS
Multistage attack	Zscaler inspects all traffic inline
Evasion technique	Zscaler has implemented instrumentation to avoid sandbox evasion
Android malware detection	Zscaler detects malicious behavior via its Cloud Sandbox

STAGES 6 & 7: COMMAND & CONTROL AND ACTION ON TARGET

If a client becomes infected with certain types of malware, the malware will try to communicate with its command and control (C&C) servers to get instructions and supply it with the victim’s data. With Zscaler, communications to C&C are intercepted and blocked by advanced threat protection engines in the Zscaler cloud using an intrusion prevention engine.

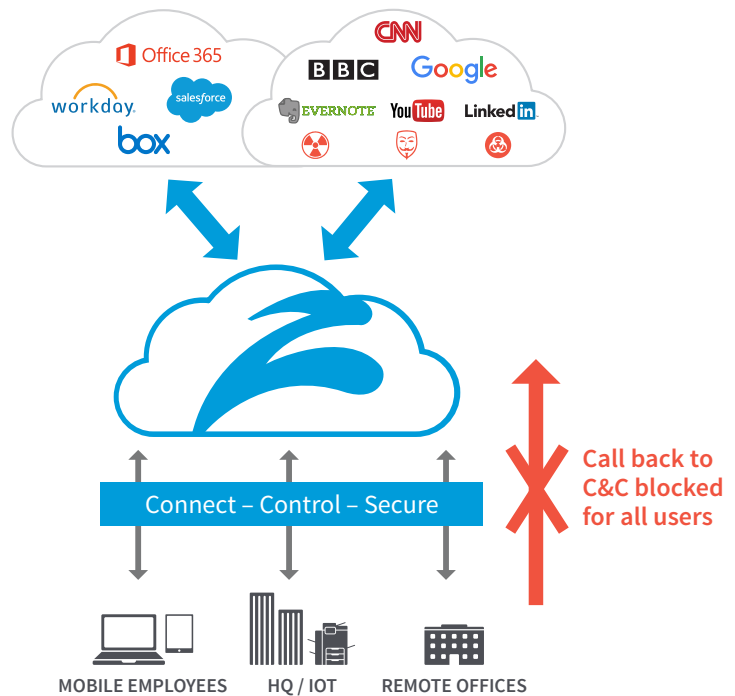


Figure 6 – Command and control communications blocked

Command & Control and Action on Target

CYBER KILL CHAIN ATTACK STAGE	KILL STEPS
C&C Communication	Zscaler blocks C&C communications via blacklist and pattern matching on the C&C

SUMMARY

While no single tool can provide 100 percent protection against APTs, the highly scalable Zscaler cloud security platform and advanced threat protection closes security gaps in your existing infrastructure to protect users against evolving threats.

The following table summarises how Zscaler disrupts the cyber kill chain.






RECONNAISSANCE	<ul style="list-style-type: none">• IP fingerprinting and scanning disrupted
DELIVERY	<ul style="list-style-type: none">• Inline analysis of dropper downloaded after exploitation• Full protection against spear phishing and water hole attacks
EXPLOITATION AND INSTALLATION	<ul style="list-style-type: none">• Inline protection against multistage attacks• Countermeasures detect evasion techniques• Mobile malware detection for Android
COMMAND AND CONTROL	<ul style="list-style-type: none">• C&C communications blocked
ACTIONS ON TARGET	<ul style="list-style-type: none">• Disrupted though Zscaler protection

CONTACT US

Zscaler, Inc.
110 Rose Orchard Way
San Jose, CA 95134, USA
+1 408.533.0288
+1 866.902.7811

www.zscaler.com

FOLLOW US

 facebook.com/zscaler
 linkedin.com/company/zscaler
 twitter.com/zscaler
 youtube.com/zscaler
 blog.zscaler.com



Zscaler™, SHIFT™, Direct-to-Cloud™ and ZPA™ are trademarks or registered trademarks of Zscaler, Inc. in the United States and/or other countries. All other trademarks are the property of their respective owners. This product may be subject to one or more U.S. or non-U.S. patents listed at www.zscaler.com/patents

©2017 Zscaler, Inc. All rights reserved. Z3426-170316