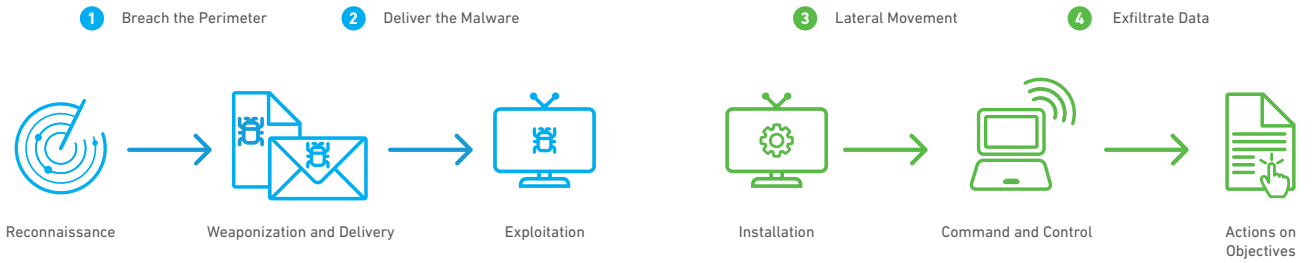
clearswift
RUAG Cyber Security

Clearswift and Cyber Kill Chain

The Cyber Kill Chain is a framework developed by Lockheed Martin[1] for the identification and prevention of cyber-attack activity. The model identifies what adversaries must complete in order to achieve their objective. Interrupt the chain, defeat the attack.



Reconnaissance

Research, identification and selection of targets, looking for publically available information on the Internet and specific technologies, with the objective to identify vulnerabilities that can be exploited.

Weaponization

The attacker uses an exploit and creates a malicious payload. Executable files and client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents can serve as the weaponized deliverables.

Delivery

The attacker delivers the malicious payload to the victim by e-mail, web, USB sticks, QR-Code, or other means. It can be the actual file, or a link which the user then clicks on.

Exploitation

Once delivered, the malicious payload is triggered either through a stealth install or through social engineering techniques and interaction with the victim. Exploits, if used, target vulnerable applications or systems within the victim's network.

Installation

Once executed, the payload installs a backdoor on the victim's system allowing persistent access to the attacker. Depending on the profile of the attack, the exfiltration of information (or encryption) can take from days to months so as not to arouse suspicion.

Command and Control

The attacker creates a command and control backdoor communication channel. This ensures the victim's servers' can communicate with the attackers, enabling a persistent "hands on keyboard access" to the target network and assets.

Actions on Objectives

The attacker takes action to achieve their goals, such as data exfiltration, data destruction, and encryption for ransom or infection of another target system or user.

[1]"Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains," Lockheed Martin Corporation.

About Clearswift

Clearswift is trusted by organizations globally to protect their critical information, giving them the freedom to securely collaborate and drive business growth. Our unique technology supports a straightforward and 'adaptive' data loss prevention solution, avoiding the risk of business interruption and enabling organizations to have 100% visibility of their critical information 100% of the time.

Clearswift operates world-wide, having regional headquarters in Europe, Asia Pacific and the United States. Clearswift has a partner network of more than 900 resellers across the globe.

More information is available at **www.clearswift.com**

UK - International HQ
Clearswift Ltd
1310 Waterside
Arlington Business Park
Theale, Reading, Berkshire
RG7 4SA

Tel : +44 (0) 118 903 8903
Fax : +44 (0) 118 903 9000
Sales: +44 (0) 118 903 8700
Technical Support: +44 (0) 118 903 8200
Email: info@clearswift.com

Australia
Clearswift (Asia/Pacific) Pty Ltd
Level 17 Regus
Coca Cola Place
40 Mount Street
North Sydney NSW 2060
Australia

Tel: +61 2 9424 1200
Technical Support: +61 2 9424 1200
Email: info@clearswift.com.au

Germany
Clearswift GmbH
Im Mediapark 8
D-50670 Cologne
Germany

Tel: +49 (0) 221 8282 9888
Technical Support: +49 (0)800 1800556
Email: info@clearswift.de

Japan
Clearswift K.K
Shinjuku Park Tower N30th Floor
3-7-1 Nishi-Shinjuku
Tokyo 163-1030
Japan

Tel: +81 (3)5326 3470
Technical Support: 0800 100 0006
Email: info.jp@clearswift.com

United States
Clearswift Corporation
309 Fellowship Road, Suite 200
Mount Laurel, NJ 08054
United States

Tel: +1 856-359-2360
Technical Support: +1 856 359 2170
Email: info@us.clearswift.com

Breaking the Cyber Kill Chain with Clearswift

Breaking the cyber kill chain at any point will defeat the attack. Multi-layer defense should be in place to do this. For most organizations this is from the delivery stage onwards. Clearswift SECURE Gateways do just this.

Clearswift SECURE Email Gateway (SEG) / Clearswift SECURE Exchange Gateway (SXG) / Clearswift ARgon for Email

- Block **Delivery** phase using Advanced Threat Protection features, sanitization of active content and dual anti-malware engines
- Block **data evasion** through email traffic as the result of **Actions on Objectives** phase using Deep Content Inspection features

Clearswift SECURE Web Gateway (SWG) / Clearswift SECURE ICAP Gateway (SIG)

- Block **Delivery** phase using Advanced Threat Protection features, sanitization of active content and dual anti-malware engines
- Block **data evasion** through HTTP/HTTPS traffic as the result of **Actions on Objectives** phase using Deep Content Inspection features

clearswift
RUAG Cyber Security