Current State of Malware Command and Control Communication Channels and Future Predictions

Fatih Ozavci
https://www.linkedin.com/in/fozavci

Executive Summary

Cyber threat actors maintain their unauthorised access to victim organisations up to years as they need long term access for cyber espionage, blockchain mining and access reselling. The malware deployed to the victims is managed through centralised systems called Command and Control (C2) servers. Whenever defence teams identify and prevent C2 servers, the threat actors are encouraged to raise the bar. Traditional tradecraft and communication channels used by threat actors are summarised in this paper with real life examples and challenges. C2 channels used in adversary simulations are also discussed such as blending into the existing corporate traffic or cloud integration. Finally, some future predictions on cyber tradecraft are provided such as distributed management infrastructure, dynamically integrating commercial services and disguising in video conferences. The techniques outlined in this paper can assist engineers to perform better exercises, collect intelligence, or build better analytics solutions.

Introduction

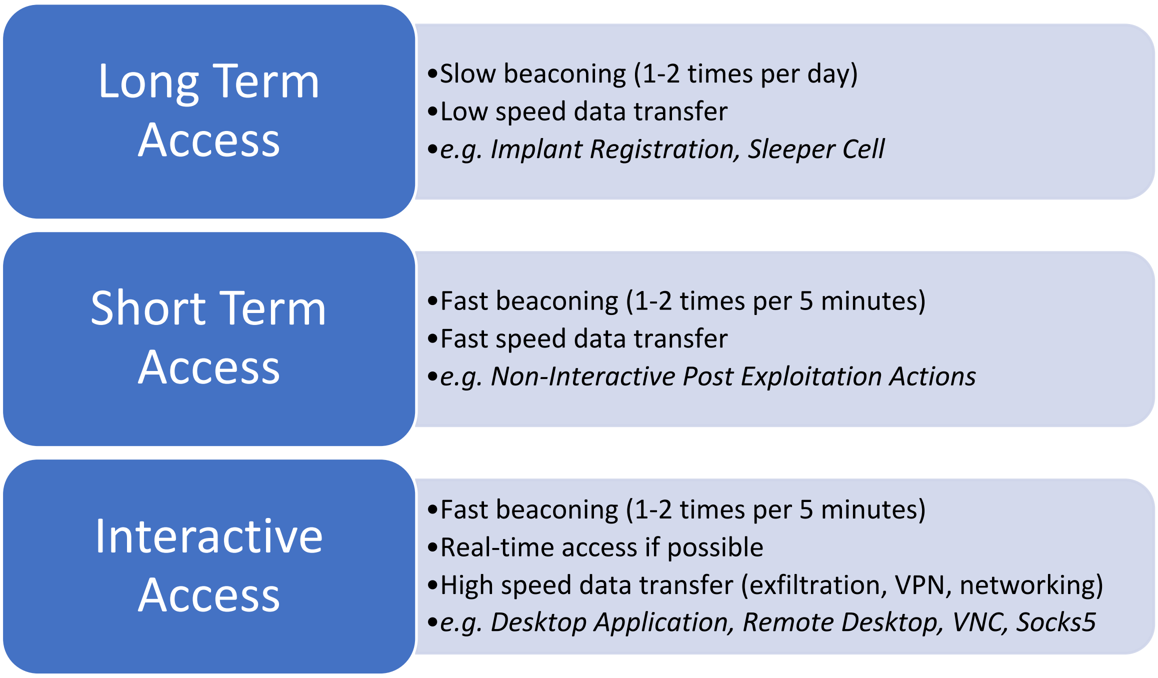
This research is focused on the C2 communication channels used by threat actors, and their current and future roles in the cyber-attacks. The communication channels used by threat actors, new techniques introduced by adversary simulation engineers, and future implementations are discussed with examples. However, the C2 and implant management design, and execution features are out of scope for this research.

Command and Control in Cyber Attacks

Criminal gangs, nation states and insiders are most common threat actors of the cyber-attacks. Threat actors run various campaigns based on their interests and motives such as extortion, cyber espionage, blockchain mining, data dealership or access reselling. In Figure 1, C2 communication channels are listed with their features and use. The C2 requirements depend on the campaign objectives and duration. While initial access resellers prefer short-term access to sell the access whenever possible, nation state actors prefer long-term access to reach the right individuals. Interactive access is also required for actions on objectives which may require real-time communications.

Advanced Threat Detection Solutions

Big data and decision analytics are widely used in cyber defence teams for threat detection and prevention. Feily et al.[1] describe the techniques which can be used to detect and prevent botnet activities. Zoldi et al.[2] also introduce malware and threat detection through cyber analytics such as determining the compromise risk with analysing DNS and IP address irregularities. Nowadays, cyber defence teams focus on integrating analytics to deep packet inspection systems, cloud monitoring and endpoint response. This encourages threat actors to improve traditional communication channels, to make the operation resilient.



Long Term Access

- Slow beaconing (1-2 times per day)
- Low speed data transfer
- *e.g. Implant Registration, Sleeper Cell*

Short Term Access

- Fast beaconing (1-2 times per 5 minutes)
- Fast speed data transfer
- *e.g. Non-Interactive Post Exploitation Actions*

Interactive Access

- Fast beaconing (1-2 times per 5 minutes)
- Real-time access if possible
- High speed data transfer (exfiltration, VPN, networking)
- *e.g. Desktop Application, Remote Desktop, VNC, Socks5*

Figure 1 Command and Control Access Types

Command and Control Communication Channels

Communication Channels Used by Threat Actors

Evasive campaign strategies would require hiding the C2 activities using unorthodox ways such as social media (e.g. Turla using Instagram[3]), stenography (e.g. Platinum using stenography[4], OceanLotus using steganography[5]) or DNS over HTTPS (e.g. APT34 using DoH[6]). Long term approach is mostly used for discovering a C2 address in case of registration, service switch or sleeping cell.

In aggressive campaigns, real-time communications are necessary for actions on objectives of the Cyber Kill Chain[7] (e.g. driving desktop applications, manual exploitation for lateral movement or seeking information). HTTP(S) is not designed as a real-time channel, therefore JavaScript or HTML5 provide this feature. The threat actors also mitigate this using SOCKS proxy (e.g. SystemBC using Socks5 Proxy[8]) or WebSocket (e.g. Magecart Skimmer using WebSocket[9]).

In certain cases, such as ransomware or air gap isolation, the threat actors implement auto driving capabilities, instead of driving through C2. Dargahi et al. [10] map the ransomware software behaviours to the Cyber Kill Chain in their research. In the research, ransomware C2 channels are mainly used for decryption key transfer or notifications, instead of driving the implant in real-time. As the threat actors use open source security software (e.g. Cobalt Strike[11], Metasploit Framework[12], PowerShell Empire[13]) to avoid attribution, they also adopt the internal network channels such as implant to implant connection through SMB Named Pipes and TCP.

Gardiner et al. [14] summarises the additional techniques used to normalise the traditional HTTP based C2 services such as evading reputation systems, controller discovery and disguising the C2 in legitimate blogs or HTML comments. However, the article is focused on detecting and preventing the C2 traffic, rather than forecasting the future techniques.

Communication Channels Used by Adversary Simulation Engineers

Adversary simulation engineers and security researchers use the threat actor techniques and tradecraft in a scenario to assess the organisations' defence against a certain actor. These scenario-based simulations follow the Cyber Kill Chain approach in general, but also adversary simulation standards where necessary such as CBEST[15] and TIBER-EU[16].

Security researchers adopt the threat actor techniques to make their simulations realistic. Though, whenever their simulations get realistic, it gets prevented by the defence teams easier due to the threat actor signatures, so the exercise objectives couldn't be achieved. As a solution, security researchers started developing various additional C2 channels to avoid detection of the main C2 channel, but also simulate the threat actor with the original technique in the threat intelligence report for exercise's sake.

While adversaries compromise legitimate web sites to use for watering hole attacks or C2 communications, researchers are not allowed to act illegal. To mitigate this, researchers register previously expired legitimate domains or domain fronting techniques. David Fifield et al. [17] describes domain fronting as a censorship circumvention technique that hides the remote endpoint of a communication. Threat actors and adversary simulation engineers use content delivery networks (CDN), and configure the malware to start call-back requests for legitimate services (e.g. Google, Microsoft or AWS services) using their TLS Server Name Indication (SNI), but communicate the real server using Host header in the HTTP request.

Security researchers also utilise cloud services to hide C2 activities such as running Cobalt Strike C2 services through AWS S3 buckets[18], serverless AWS Lambda applications used as a redirector[19] and utilising task feature of Microsoft Outlook in Office 365[20]. F-Secure also developed a project called Custom Command and Control (C3)[21] which allows researchers to utilise various legitimate web services, cloud infrastructure and network protocols as communication channels.

Furthermore, new protocols such as HTTP 2, HTTP 3 and DNS over HTTPS are also used for C2 communications by engineers and threat actors. Merlin C2[22] supports HTTP 2 and 3 protocols with QUIC protocol as C2 communications channel. Godoh C2[23] is also proof of concept solution to demonstrate the DNS over HTTPS use for C2 communications. Most of the deep packet inspection and network/proxy security inspection solutions have limited capability to understand and intercept these protocols. Through this, the adversaries and engineers are able to drive their implants.

Infection Monkey[24] is designed to infect victims in scope automatically using a decision flow. It's useful to assess the defence solutions and generate indicators of compromise (IoC) in a limited scope. However, it's not used for threat actors or offensive adversary simulations due to well-known signatures. It still represents a new milestone for automating infections without waiting for C2 instructions.

Academic Research on Adversary Simulations

The Mitre Att&ck framework[25] describes most used C2 communication types such as various network protocols, multi stage channels, encryption, web services and application layer protocols. Strom at al. [26] introduce using data analytics for the C2 detections such as downloading second stage payload, or social media channels while describing the Mitre Att&ck framework, analytics and scenario development.

In addition, Applebaum et al. [27] [28] [29] [30] introduce various adversary emulation techniques and implementations in their research. The simulations used for research are based on Mitre CALDERA[31] framework, and mainly focused on endpoint, lateral movement and post-compromise activities. Recently, Yoo et al.[32] also released a research for adversary emulations describing scenario automations using a custom red team implant instead of Sandcat of CALDERA.

However, common challenge of these academic research projects is limited simulations of the C2 channels. The implants were mainly using HTTP(S), and also some common protocols (e.g. DNS). This is not a good coverage of the C2 communications, so the defence systems and analytics implementations wouldn't be trained effectively. This creates an opportunity for the threat actors to use uncommon techniques to avoid detection for the evasive campaigns.

Future of Resilient Communication Channels

Threat actors improve their tradecraft where the defence solutions start preventing them. Due to emerging cyber analytics use, HTTP profile changes and domain fronting are not sufficient anymore. Distributed infrastructure approach likely to be used for managing larger and detection resilient campaigns.

In a distributed infrastructure as outlined in Figure 2, the threat actor can utilise the legitimate Internet services for implant communications. The infrastructure can be deployed automatically, and per campaign, using the cloud automation tools, API support of the social media services, data hidden in images with stenography and news site comments. Data transmission should be also encrypted per implant to make the infrastructure resilient to defence activities for months. It's also scalable and easier to add new services to various categories.

The minimized implant would run a series of discovery actions to find a reachable registration service. After registration, it would adjust the check-in frequency, and load modules when necessary. Interactive services also could be utilised through video conference solutions. Finally, the data exfiltration stage would use interactive services or slow upload features depending on the data size. In case of detection, the infrastructure would survive longer, but also it would be possible to add new services to defend it against aggressive defence teams.

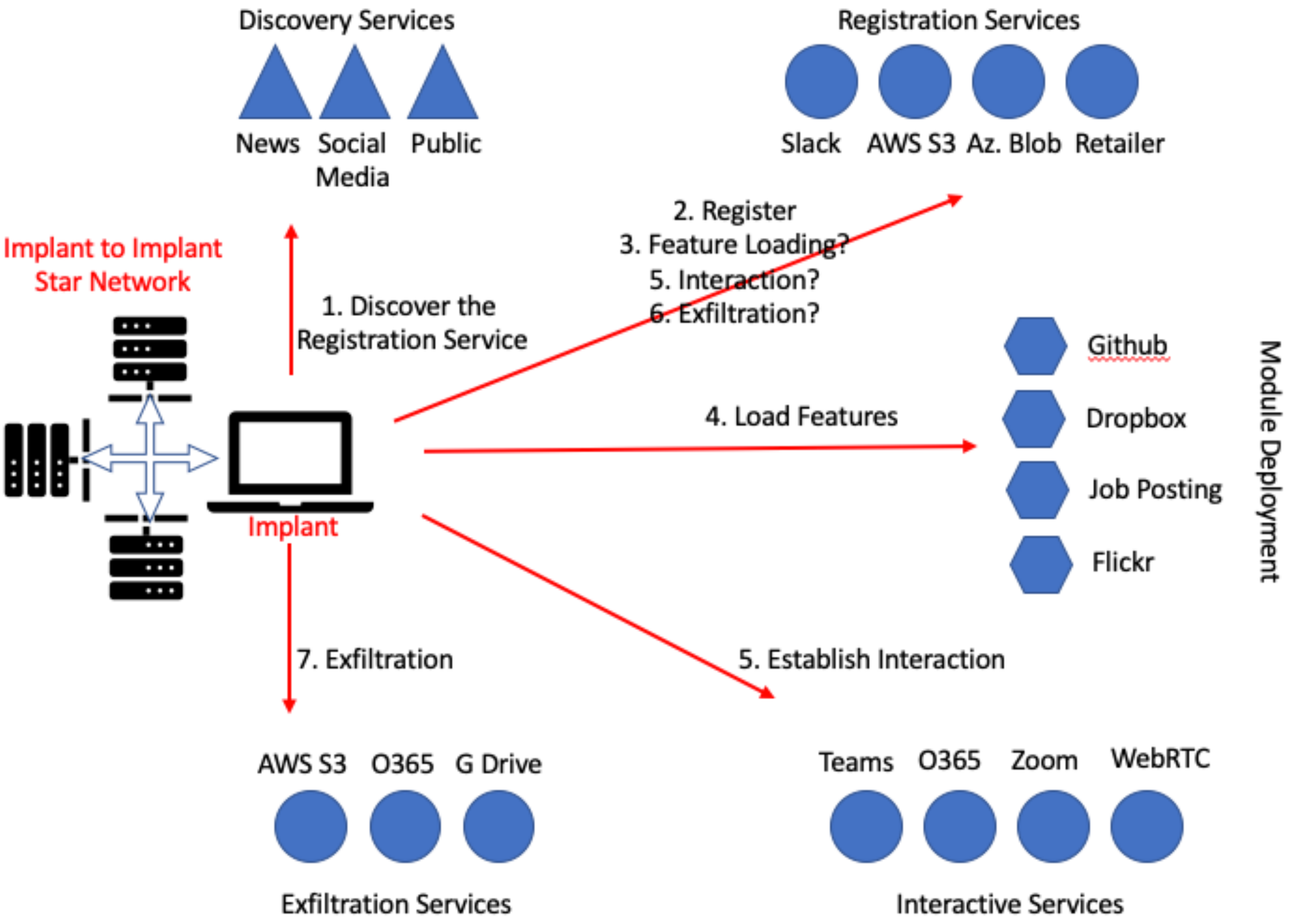


Figure 2 Distributed C2 Infrastructure Using Legitimate Services

Web Real-Time Communications (WebRTC) provides a real-time communication channel with various transport options (audio/video conferences). The threat actors use it only for revealing the victim IP addresses while targeting. There is still no WebRTC implementation used by a threat actor, such as hiding instructions in audio streams or events through commercial video conference services. QUIC implementation of Merlin C2 is not used by threat actors either, only simulations. When defenders implement a good analytics coverage on HTTP based C2 channel detection, the newer protocols (e.g. WebRTC, QUIC) which run on HTTP will find their use in cyber-attacks.

Utilising advanced decision-making process would also make difference. The implants should be lightweight, so artificial intelligence (AI) or machine learning (ML) are not. The initial implant can load it remotely (or use public AI APIs) where campaigns run with less interaction. Infection Monkey style exploit automation would also improve the nation-state campaigns. The implants would use a star network to operate autonomously where internet isn't an option, and share it if an implant discovers access to the distributed infrastructure.

Conclusion

Traditional C2 communication channels are easier to detect, and this gets easier with cyber analytics every day. Therefore, threat actors and adversary simulation engineers improve the communication channels to get better defence evasion. Customised HTTP profiles and domain fronting, and cloud integration, would be sufficient for today. Though, in near future, they need to improve their infrastructure with distributed management, video conference solutions, newer HTTP implementations and decision-making automation.

References

[1] Feily, M., Shahrestani, A., & Ramadass, S. (2009, June). A survey of botnet and botnet detection. In *2009 Third International Conference on Emerging Security Information, Systems and Technologies* (pp. 268-273). IEEE.

[2] Zoldi, S., Athwal, J., Li, H., Kennel, M., & Xue, X. (2015). *U.S. Patent No. 9,191,403*. Washington, DC: U.S. Patent and Trademark Office.

[3] ESET, " *Cyber espionage group, Turla, new campaign uses Instagram to spy on its targets*" June 2017. [Online]. Available: https://www.eset.com/us/about/newsroom/press-releases/cyber-espionage-group-turla-new-campaign-uses-instagram-to-spy-on-its-targets/. [Accessed 8 September 2020].

[4] Kaspersky, "*Platinum is back*" June 2019. [Online]. Available: https://securelist.com/platinum-is-back/91135/ [Accessed 8 September 2020].

[5] Blackberry Cylance, "*OceanLotus APT Group Leveraging Steganography*" February 2019. [Online]. Available: https://securelist.com/platinum-is-back/91135/ [Accessed 8 September 2020].

[6] ZDNet, "*Iranian hacker group becomes first known APT to weaponize DNS-over-HTTPS (DoH)*" August 2020. [Online]. Available: zdnet.com/article/iranian-hacker-group-becomes-first-known-apt-to-weaponize-dns-over-https-doh/ [Accessed 8 September 2020].

[7] The Cyber Kill Chain by Lockheed Martin. [Online]. Available: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html. [Accessed 10 September 2020].

[8] ThreatPost, "*Brand-New SystemBC Proxy Malware Spotted Using SOCKS5 for Stealth*" August 2019. [Online]. Available: https://threatpost.com/systembc-proxy-malware-socks5-stealth/146879/ [Accessed 10 September 2020].

[9] MalwarebytesLabs, "*New evasion techniques found in web skimmers*" January 2020. [Online]. Available: https://blog.malwarebytes.com/threat-analysis/2019/12/new-evasion-techniques-found-in-web-skimmers/ [Accessed 10 September 2020].

[10] Dargahi, T., Dehghantanha, A., Bahrami, P. N., Conti, M., Bianchi, G., & Benedetto, L. (2019). A cyber-kill-chain based taxonomy of crypto-ransomware features. *Journal of Computer Virology and Hacking Techniques*, *15*(4), 277-305.

[11] Strategic Cyber LLC, a HelpSystems company, "*Cobalt Strike*". [Online]. Available: https://www.cobaltstrike.com/ [Accessed 10 September 2020].

[12] Rapid 7, "*Metasploit Framework*". [Online]. Available: https://www.metasploit.com/ [Accessed 10 September 2020].

[13] "PowerShell Empire". [Online]. Available: https://www.powershellempire.com/ [Accessed 10 September 2020].

[14] Gardiner, J., Cova, M., & Nagaraja, S. (2014). Command & Control: Understanding, Denying and Detecting-A review of malware C2 techniques, detection and defences. *arXiv preprint arXiv:1408.1136*.

[15] Bank of England, " *CBEST Intelligence-Led Testing Implementation Guide*" 2016. [Online]. Available: https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/cbest-implementation-guide.pdf [Accessed 10 September 2020].

[16] European Central Bank, " *TIBER-EU FRAMEWORK How to implement the European framework for Threat Intelligence-based Ethical Red Teaming*" May 2018. [Online]. Available: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf [Accessed 10 September 2020].

[17] Fifield, D., Lan, C., Hynes, R., Wegmann, P., & Paxson, V. (2015). Blocking-resistant communication through domain fronting. *Proceedings on Privacy Enhancing Technologies*, *2015*(2), 46-64.

[18] Rhino Security Labs, "*Hiding in the Cloud:*
Cobalt Strike Beacon C2 using Amazon APIs". [Online]. Available: https://rhinosecuritylabs.com/aws/hiding-cloudcobalt-strike-beacon-c2-using-amazon-apis/ [Accessed 10 September 2020].

[19] Adam Chester, " *AWS Lambda Redirector*" February 2020. [Online]. Available: https://blog.xpnsec.com/aws-lambda-redirector/ [Accessed 10 September 2020].

[20] F-Secure, MWR Labs, " *“Tasking” Office 365 for Cobalt Strike C2*" September 2017. [Online]. Available: https://labs.f-secure.com/archive/tasking-office-365-for-cobalt-strike-c2/ [Accessed 10 September 2020].

[21] F-Secure, MWR Labs, " *Custom Command and Control*" September 2017. [Online]. Available: https://labs.f-secure.com/tools/c3/ [Accessed 10 September 2020].

[22] Merlin, "*Merlin Command and Control Server*". [Online]. Available: https://github.com/Ne0nd0g/merlin [Accessed 10 September 2020].

[23] Godoh, " *A DNS-over-HTTPS Command & Control Proof of Concept*". [Online]. Available: https://github.com/sensepost/godoh [Accessed 10 September 2020].

[24] Guardicore, "*Infection Monkey Features*". [Online]. Available: https://www.guardicore.com/infectionmonkey/features.html [Accessed 10 September 2020].

[25] The MITRE Corporation, "*Adversarial Tactics, Techniques and Common Knowledge*," September 2020. [Online]. Available: https://attack.mitre.org/. [Accessed 8 September 2020].

[26] Strom, B. E., Battaglia, J. A., Kemmerer, M. S., Kupersanin, W., Miller, D. P., Wampler, C., ... & Wolf, R. D. (2017). Finding cyber threats with ATT&CK-based analytics. *The MITRE Corporation, Bedford, MA, Technical Report No. MTR170202*.

[27] Applebaum, A., Miller, D., Strom, B., Korban, C., & Wolf, R. (2016, December). Intelligent, automated red team emulation. In *Proceedings of the 32nd Annual Conference on Computer Security Applications* (pp. 363-373).

[28] Musman, S., Booker, L., Applebaum, A., & Edmonds, B. (2019, May). Steps toward a principled approach to automating cyber responses. In *Artificial Intelligence and Machine Learning for Multi-Domain Operations Applications* (Vol. 11006, p. 110061E). International Society for Optics and Photonics.

[29] Applebaum, A., Miller, D., Strom, B., Foster, H., & Thomas, C. (2017, July). Analysis of automated adversary emulation techniques. In *Proceedings of the Summer Simulation Multi-Conference* (pp. 1-12).

[30] Miller, D., Alford, R., Applebaum, A., Foster, H., Little, C., & Strom, B. (2018). Automated adversary emulation: A case for planning and acting with unknowns. *MITRE: McLean, VA, USA*.

[31] The MITRE CALDERA, September 2020. [Online]. Available: https://github.com/mitre/caldera. [Accessed 8 September 2020].

[32] Yoo, J. D., Park, E., Lee, G., Ahn, M. K., Kim, D., Seo, S., & Kim, H. K. (2020). Cyber Attack and Defense Emulation Agents. *Applied Sciences*, *10*(6), 2140.