CND Equities Strategy

Jonathan M. Spring, Edward Stoner
CERT® Division, Software Engineering Institute
Carnegie Mellon University
netsa-contact@cert.org
Publication CERTCC-2015-40

July 2015

1 Introduction

The goal of computer network defense (CND) is to protect the system and ensure the organization operates resiliently under strain [1]. To succeed, the CND strategy must plan for adversary response to defensive measures. Part of this planning is strategic management of equities.

In the security field, the word *equities* has a special meaning: information assets that provide an advantage over the adversary, especially where the owner is confident the adversary does not know of those assets. Examples of equities include a clandestine informant or details of adversary tools, tactics, or procedures (TTPs) that facilitate attribution [2], detection, or prevention [3]. To *destroy* or *burn* equities is to render information assets useless by disclosure to the adversary.

To defend a network, the CND operator must reveal some information. When an operator blocks a command and control (C2) domain name or IP address, the adversary will almost certainly notice that their tool stops communicating. Likewise with cleaning an infected system. So the question is not whether to reveal equities, but which equities to reveal and which to hold in reserve at what times to gain maximum advantage. We can use game theory to model this via information states [4], but this short paper will stick to a more friendly and informal discussion.

CND methods can leverage either *robust* or *fragile* equities. Whether an equity is robust or fragile is based on a simple question:

How will the adversary respond to learning of the information asset?

An equity is robust if the adversaries must make expensive or difficult changes to their TTPs in response to the CND method despite gaining knowledge of the revealed information, and these changes are relatively easy for the operator to continue detecting.

An equity is fragile if the adversaries can make a quick or simple change to their TTPs that will still allow them to reach their intrusion objective (financial gain, political gain, or damage [5, p. 15]), and this change in TTPs will be relatively hard for the CND operator to detect and update their information assets.

A CND operator can and should use both robust and fragile equities. Fragile equities are not inherently worse. Fragile equities may be cheaper to maintain or used to gather intelligence without revealing them. The distinction between fragile and robust equities is relevant when determining what to block, share with trusted parties, or publicize.

The CND operator should think about what the adversary is going to do in response to CND methods and enact those methods that will force a favorable TTP change by the adversary. The following examples demonstrate this point.

2 Examples

The following are examples of well-known CND methods. For each example, we answer the question presented in Section 1, "How will the adversary respond?" and analyze the answer to describe why each example is either robust or fragile. Since these examples are well known, we generally do not have to speculate about adversary responses, but we can use past experience to confirm our expectations. Robust examples are blocking scanning IP addresses and blocking fast-flux domain networks. A fragile example is relying on access to cleartext for IDS (Intrusion Detection System) signatures.

2.1 Robust Detection Equities

Scanning is behavior seeking information about a target by sending probing traffic [6, see: probe]. Effective tools are free and open source [7]. Although it is cheap, an adversary usually needs to scan many locations. Most scanning is brute-force: just try everything. Therefore, an adversary wants to scan quickly and at high volume, otherwise the scan will not finish in a useful amount of time and intrusion objectives will not be met.

How will an adversary respond if the CND operator blocks scanning IPs or publishes scanning IPs? The adversary's scanning technique will have to change to avoid detection. Detection is usually based on a combination of packet contents, traffic volume, and source addresses. There are many well-known scans that use malformed packets, but if they are blocked then the adversary cannot learn anything using these scans. The adversary cannot change TTPs to gain the same information in many cases; blocking such malformed packets uses robust equities (the information asset is the list of malformed packet patterns).

Many scans use well-formed packets, but in high volume from a small set of sources. If the defender blocks these sources and publishes them so others can also prevent scans from them, then the adversary must reduce their scanning rate to avoid detection. The information asset that could be blocked and/or shared in this case is source IP addresses that commit suspicious scans. This response undermines the adversary's goal, as scans will not complete in a useful amount of time. Adversaries could still scan certain targets slowly, but defenders continually improve their scan detection and further reduce adversary scan throughput by further blocking and publishing the offending sources, and therefore is robust.

Fast-flux networks are service delivery networks that change DNS entries quickly to provide reliable service to malicious networks [8]. The individual domains or IP addresses in a fast-flux network are fragile equities: the adversary has built in the ability to cheaply change them. However, the defender can detect a fast-flux network per se and prevent communications using any fast-flux network [9]. The information asset of detecting fast-flux behavior is robust. The detection depends on quick DNS changes, so the adversary's only response is to slow down or avoid the DNS. Slowing down makes their delivery network more fragile, which is favorable to the defender. Avoiding the DNS requires major redevelopment of stable infrastructure, which also favors the defender.[1]

2.2 Fragile Detection Equities

A network-based IDS often relies on signatures to detect suspicious traffic [3]. Signatures are not inherently either fragile or robust. However, an instructive example comes from the case of signatures relying on specific patterns within the packet payload. Initially, malicious traffic was sent in cleartext – i.e., readily readable by any device that handled the network traffic. Defenders developed IDS signatures based on patterns within this cleartext.

[1] Adversaries eventually learned to avoid the DNS via peer-to-peer networks; a discussion of detecting P2P traffic is beyond the scope of this paper.

So, "how will the adversary respond?" Simply, the adversary encrypts the traffic so the cleartext is not visible. Sometimes the adversary uses standard encryption suites like TLS (Transport Layer Security) and AES (Advanced Encryption Standard), but what algorithm is used does not matter to the IDS signature. A trivial encryption like a Caesar cipher could be used, and the IDS signature would not work unless the encryption is detected and broken before applying the signature. Breaking encryption does not scale for the defender, and applying encryption is trivial because so many open source libraries exist to do various methods. Therefore, IDS signatures of cleartext packet payloads are fragile equities.

3 Conclusion

The basic strategy for the CND operator has two parts. First, do not reveal fragile equities to the adversary. Second, for CND methods that reveal equities, create and use robust equities. In all cases, plan for how the adversary will respond to defensive measures.

Acknowledgements

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

DM-0002601

References

[1] Fisher D, Linger R, Lipson H, Longstaff T, Mead N, Ellison R. Survivable Network Systems: An Emerging Discipline. Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University; 1997. CMU/SEI-97-TR-013. Available from: http://resources.sei.cmu.edu/library/asset-view.cfm?AssetID=12905.

[2] Caltagirone S, Pendergast A, Betz C. The Diamond Model of Intrusion Analysis. Center for Cyber Intelligence Analysis and Threat Research; 2013. Available from: http://www.threatconnect.com/methodology/diamond_model_of_intrusion_analysis.

[3] Scarfone K, Mell P. Guide to intrusion detection and prevention systems (IDPS). National Institute for Standards and Technology; 2007. 800-94. Available from: http://csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf.

[4] Spring JM. Toward Realistic Modeling Criteria of Games in Internet Security. Journal of Cyber Security & Information Systems. 2014;2(2):2–11. Available from: http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=312713.

[5] Howard JD, Longstaff TA. A common language for computer security incidents. Sandia National Laboratories; 1998. SAND98-8667. Available from: http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.31.4289.

[6] Shirey R. Internet Security Glossary, Version 2. IETF; 2007. RFC 4949 (Informational). Available from: http://www.ietf.org/rfc/rfc4949.txt.

[7] Lyon GF. Nmap Network Scanning: The Official Nmap Project Guide To Network Discovery And Security Scanning. Nmap Project; 2011.

[8] Salusky W, Danford R. Know Your Enemy: Fast-Flux Service Networks. The Honeynet Project; 2007. Available from: http://www.honeynet.org/papers/ff/.

[9] Holz T, Gorecki C, Rieck K, Freiling FC. Measuring and Detecting Fast-Flux Service Networks. In: Proceedings of the 15th Annual Network and Distributed System Security Symposium; 2008. Available from: http://pi1.informatik.uni-mannheim.de/filepool/publications/fast-flux-ndss08.pdf.