



The Cybersecurity Think Tank

Signature Based Malware Detection is Dead

February 2017

Author: James Scott (Senior Fellow – Institute for Critical Infrastructure Technology)

Contents

Introduction	4
Antiquated Technologies are No Match for Today's Cyber-Adversaries.....	6
The Rise of Artificial Intelligence.....	9
Does Not Compute.....	10
Conclusion.....	12
ICIT Contact Information.....	14
Sources.....	15

Signature Based Malware Detection is Dead

February 2017

Author

James Scott, Sr. Fellow, ICIT

Copyright © 2017 Institute for Critical Infrastructure Technology – All Rights Reserved

Upcoming Event

Join us at the 2017 Critical Infrastructure Forum to learn about the findings in this research paper.



www.ICITForum.org

**Visit the ICIT Library to view additional
research and publications**

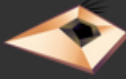
https://www.amazon.com/James-Scott/e/B01IPLQKSO/ref=dp_byline_cont_pop_ebooks_1


Introduction

Signature and behavioral based anti-malware are no match for next generation adversaries who utilize mutating hashes, sophisticated obfuscation mechanisms, self-propagating malware, and intelligent malware components. It is no longer enough to detect and respond. Artificial intelligence offers the predictive quality that can give organizations a much-needed edge on their more sophisticated, less burdened, and more evasive adversaries. In 2016, organizations whose cybersecurity was merely the public display of Security Theater were pummeled directly and indirectly by unknown adversaries. Some organizations discovered the breaches and initiated incident response, while most others remain ignorant of the fact that their networks are actively pulsating with threat actors, who set up beachheads for future attack and who exfiltrate treasure troves of valuable data. The average breach results in a cost of \$158 per stolen record and is often not detected for an average of 229 days [1]. In that time, cyber threat actors exhaust the network of valuable data, capitalize further by selling network access as a service and further victimizing the organization, and laterally transition onto associated networks using the data or access garnered from the breach. The "detect and respond" cycle must end. Critical infrastructure organizations cannot afford to suffer another Anthem or Target style breach. National Security cannot withstand another OPM. Critical infrastructure organizations need the advantage afforded from the adoption of sophisticated machine learning based artificial intelligence that depends on complex algorithms to detect, prevent, and mitigate malicious files and code prior to execution, based on their characteristics.


Figure 1: HackForums Sale of “FUD” (Fully-Un-Detectable) Agent Tesla Keylogger

11-04-2014, 12:23 PM (This post was last modified: 11-04-2014 12:32 PM by agent_tesla.)



agent_tesla 

agenttesla.com

 **L33T**

```

[img]http://i.hizliresim.com/Ml3rkN.png[/img]
[img]http://i.hizliresim.com/Qgo9Qk.png[/img]
[img]http://i.hizliresim.com/XYr597.png[/img]
[img]http://i.hizliresim.com/b4dWk8.png[/img]
[img]http://i.hizliresim.com/dqAR84.png[/img]
[img]http://i.hizliresim.com/5R1BLR.png[/img]
[img]http://i.hizliresim.com/AYdpn0.png[/img]
[img]http://i.hizliresim.com/02oQl8.png[/img]

Result: (0/60)
A-Squared(Emisoft AntiMalware) Clean - Nothing Found
Agnitum Clean - Nothing Found
AhnLab V3 Internet Security Clean - Nothing Found
ArcaVir Clean - Nothing Found
Avast Clean - Nothing Found
Avg Clean - Nothing Found
Avira Clean - Nothing Found
Ad-Aware Clean - Nothing Found
Baidu AV Clean - Nothing Found
BitDefender Clean - Nothing Found
BKav Clean - Nothing Found
BullGuard Internet Security Clean - Nothing Found
ByteHero Clean - Nothing Found
ClamAv Clean - Nothing Found
Comodo Clean - Nothing Found
Dr. Web Clean - Nothing Found
eScan Clean - Nothing Found
eTrust-Vet Clean - Nothing Found
eScan Internet Security Suite 14 Clean - Nothing Found
ESET NOD32 Clean - Nothing Found
Fortinet Clean - Nothing Found
Fprot Clean - Nothing Found
FSB Antivirus Clean - Nothing Found
F-Secure Clean - Nothing Found
Gdata Clean - Nothing Found

```



Figure 1 depicts a Hackforums sale of the Agent Tesla keylogger. The poster claims that the keylogger cannot be detected by any of the signature, heuristic, and behavior based anti-virus programs listed.

Antiquated Technologies are No Match for Today's Cyber-Adversaries

For over a decade, cybersecurity has been a game of “detect and respond” or “breach and react.” Public and private sector budgets have been inefficiently squandered on antiquated and ineffectual security solutions that continuously fail to protect critical data resources from sophisticated and unsophisticated cyber-adversaries alike. As the ease of compromise and the sophistication and population of cyber-threats increased, organizations were forced to rely on

more and more layers of inter-connected vendor-supplied security solutions in order to protect users, networks, data centers, and cloud resources. These legacy endpoint solutions require constant updating, maintenance, and signature generation; though, many of the vendors no longer provide service for those products or are no longer in service themselves. More modern solutions, that automatically and continuously update are also ineffective against modern threats because they do not protect against targeted or novel attacks. Information technology and information security personnel are inundated by the number of dashboards, products, and security suites necessary to minimally protect vital infrastructure. In critical infrastructure sectors especially, layers of incompatible technologies are “Frankensteined” together in a haphazard attempt at nominally meeting security standards. Any unused technology in every layer exponentially increases cybersecurity noise and could result in exploitable security vulnerabilities. Meanwhile, C-level executives suffer from security solution fatigue as the result of incessant product evaluations, investments, and failures.

Figure 2: Hansa Market FUD RAT Listing

The screenshot shows the Hansa Market interface for a RAT4A v.1.0 (Spy On Cam) listing. The page header includes the Hansa logo and navigation links for Home, Forums, Support, Login, and Register. The listing itself features a screenshot of the RAT's interface, which includes a table with columns for Device ID, Manufacturer, Model, Product, Service, App, Network, Database, NetworkType, PhoneType, and OSVersion. The price is listed as USD 1.10 (0.0011 BTC) and is marked as 'In stock'. The vendor is 'shonajaan' with a phone number [+177]-22 and a Level 6 (400+) rating, and is labeled as a 'Trusted Vendor'. The class is 'Digital' and the delivery is 'Instant Delivery'. A 'Buy Now' button is prominently displayed, along with 'Question' and 'Report' options. Below the listing, there are 'Details' and 'Feedback' buttons. The 'Listing Details' section lists the following features: Reverse connection, Remote cam (back/front), Remote chat, Geolocalized, File manager, Remote Shell, Audio recording, Micro spy, SMS Stealer, and FUD.

Figure 2 displays a Fully Un-detectable (FUD) Remote Access Trojan (RAT) sold on Hansa Market. Buyers look for the FUD keyword because it signifies that the malware will not be detected by signature or behavior based anti-malware applications.

Cyber-adversaries and information security professionals are perpetually engaged in a fierce cyber-arms race focused around the access and exfiltration of the sensitive data contained in critical infrastructure systems. The asymmetric nature of the cyber-threat landscape pre-positions attackers ahead of information security personnel. Attackers can dedicate all their resources towards innovation and development while organizations must maintain and defend their assets. As a result, it is paramount that only the most efficient, powerful, and cost-effective security solutions are implemented in critical infrastructure cyber-defense. Most detection and reactionary machine learning endpoint security solutions are now obsolete because adversaries can easily mutate their malware or trivially generate new malware before the antiquated AI can recognize or respond to the threat. Without defense-grade, machine learning artificial intelligence cybersecurity solutions, critical infrastructure will inevitably lose the hyper-evolving battle for cyber-space. Malware is actively adapting to include more sophisticated components. At least one virus, Zeliome, already roughly included AI capabilities. Another malware uses AI to alter its signature, to regulate its activities, to generate lures, to self-propagate, to strategically deliver other malware, and to maximize its damage while minimizing its footprint [2]. These features are becoming more common in malware while innovative AI cybersecurity is dwindling as a result of “silver-bullet” solution vendors peddling antiquated solutions instead of relying on more sophisticated characteristic based machine learning artificial intelligence. Nearly every new malware includes intelligent deception, obfuscation, and evasion components [3].

Figure 3: Hansa Market FUD Guide

The screenshot shows a product listing on the Hansa Market website. The product title is "How to Create a FUD Backdoor Bypass Antivirus". The price is listed as USD 1.00 and ₱ 0.0010. The item is marked as "In stock". The vendor is "I33ter [+1636]-34" with a Level 9 (3000+) and a "Trusted Vendor" badge. The class is "Digital" and the delivery is "Instant Delivery". There is a "Buy Now" button and a "Quantity" input field set to 1. Below the product image, there are tabs for "Details" and "Feedback".

Listing Details

This tutorial will teach you How to Create a FUD Backdoor and Bypass Antivirus

Figure 3 features a Hansa Market guide that script kiddies purchase when attempting to make their malware undetectable to Anti-virus applications.


The Rise of Artificial Intelligence

Some of the first attempts at Artificial Intelligence began in the 1950s with the invention and application of machine learning algorithms meant to mimic a brain's neural network and human biology. Artificial intelligence is a measure of the quality and capability of the applications and of the machine learning algorithms employed. Machine learning is a sub-process of artificial intelligence that enables computer applications to learn and adapt based on new data, without needing to be explicitly programmed to adapt or to respond. "Weak" AI is able to solve minor creative tasks, recognize images, predict weather patterns, play games, etc.; meanwhile, "strong" AI is capable of thinking, of understanding, and of solving tasks other than what it was programmed for. Advances in machine learning have already defined innovation in the healthcare, financial, manufacturing sectors, and its influence in other critical infrastructure sectors is undeniable. Attempts at applying machine learning algorithms to cybersecurity began in the 2000's; however, the implementation often relied on signatures and heuristics and almost always required human interaction [4]. Signature based detection is not scalable when there are hundreds of new signatures every day, let alone when there are hundreds of thousands [1]. Now, with the daily creation of nearly one million new malware, signature based and heuristic based anti-malware is insufficient [5]. Critical infrastructure cybersecurity needs a quantum leap forward. It needs to rely on sophisticated and innovative machine learning based artificial intelligence anti-malware solutions that do not operate based on signatures or heuristics. Many "silver-bullet" vendors offer faux-AI solutions that operate on imprecise algorithms, that do not draw from large enough data pools, or that do not analyze files according to enough features. These solutions cannot precisely evaluate files at a granular level. Other, worse solution providers tout machine learning capabilities, but really only offer the application of "exception"-derived signatures to generic templates.

Figure 4: HackForums Script Kiddie FUD Discussion

FUD RAT or FUD Crypter Thread Options

05-14-2012, 12:44 PM Post: #1

 Android Developer Prestige: 50
Posts: 403
Joined: Jan 2009
Reputation: 69


hey guys,

What do you think is best? A **FUD** RAT or a Rat crypted from a **FUD** Crypter???


.PHAETHON

PM Find TS Quote Q+ Report

05-14-2012, 12:45 PM Post: #2


 **InfectedWorld** Prestige: 208
Posts: 2,326
Joined: Dec 2010
Reputation: 317

LEROOOOOY JENKIIINS

 **UB3R**

A **FUD** rat because there is no cost to buy a crypter or time to make one but they will not last long because most RATS are overused

03-31-2013, 05:35 AM (This post was last modified: 03-31-2013 05:39 AM by a0rta.) Post: #4

 [closed@HF:] Prestige: 0
Posts: 6
Joined: Mar 2013
Reputation: 0

LMFAO. Wrote: (05-14-2012 12:46 PM)

I don't think you can have a **FUD** RAT. A RAT is a Remote Administration Tool. Any RAT that you buy is "supposed" to be used for network management, etc., so they wouldn't make it **FUD**.

Anti-virus is meant to pick up RATs and block them by default. So a **FUD** crypter would be your only option.

Someone please correct me if I'm wrong. :)

That doesnt say that one cant make a **fud** RAT.

It's all depending on what purpose it's made for and the major part of RAT's out there isn't **fud** due to that they have been over used but if someone makes their own RAT it can for sure be made **fud**. The question would rather be for how long will it stay **fud**?

For that reason I would go for a **fud** crypter rather then a **fud** RAT as it helps one more when spreading the RAT. It's also a lot easier to get a new crypter then have to make a RAT **fud** again when caught by antivir.

...ops... just saw that this was an kind of old post I responded to. :(

PM Find TS Quote Q+ Report

Figure 4 captures a Hackforums discussion of FUD malware development. Notice that the participants do not argue whether antivirus can be avoided so much as they discuss how to avoid it and what malware is a better investment. Script kiddies and more sophisticated attackers long ago accepted the flaws in signature and behavioral-based detection. It is time for the information security community to phase out antiquated AV models and adopt characteristic-based AV that is complimented by a sophisticated AI platform.

Does Not Compute

Marketable machine learning anti-malware applications can detect entire families of malware despite numerous modifications and it can be developed to detect future variations and threats. However, small "mini-families" cannot be taught to an AI that relies on generalization machine learning algorithms because the sample size necessary to adapt to detect the threat is

too small. In these cases, most products revert to a detection layer based on signatures, hashes, masks, etc. Similarly, targeted malware is authored by threat actors who do not intend to mutate their samples or wildly propagate their malware. As a result, the single malware sample served to the single victim bypasses most protection solutions unless it is somehow detected by a layer of antiquated hash or signature detection. Critical infrastructure cannot withstand targeted attacks that bypass inefficient security solutions. Instead, critical infrastructure organizations need to rely on more advanced AI protection solutions that detect malware based on the characteristics of malicious files and code, prior to execution or transmission.

Figure 5: HackForums Signature Anti-Virus Evasion Tutorial

THIS SOME METHODES I COLLECT THEM FROM THE NET MAY HELP
SOMEONE
By THE_METALISME_AGAIN

In this tutorial I will be showing you 4 ways of how to make a Trojan undetectable to Anti-Virus software. I am sure there are more then 4, but these should help get you started.

1. Encrypters/Compressers:

You would think this should be the easiest way to UD (Undetect) a Trojan...but alas, it is not. The problem is simply this, most people use the same Trojans and Packers so often that Anti-Virus software knows pretty much all the signatures. They either use Ardamax Keylogger, Optix Pro, Beast, ProRat etc. for Trojans. For Packers they use UPX, PECompress, AsPack, Mophine etc. Again, none of these combinations work because all the signatures have been flagged. The best way this option will work is to find lesser known Packers and Trojans to work with.

Try a Google search for Executable Packers. Get a few that you have not heard of before or that have a decent rating. If it is not freeware, I am sure there will be a Crack for it. For Trojans, three good resources are VXChaos, LeetUpload or VX Heaven. Remember to pick the ones that are not well known and try to mix and match those Trojans and Packers.

2. Byte Adders:

This technique allows you to add junk bytes to your Trojan as to confuse Anti-Virus software. It does this by moving the code around inside the executable as the bytes are being added. This means that the signature will not be in the place the Anti-Virus expects it to be. A good tool for this would be StealthTools v2.0 by Gobo.

3. Hex Editing:

This is much more complicated and takes a lot more practice to get right. The idea here is to find the signature that Anti-Virus software has flagged inside of your Trojan and change it by adding a different byte, or changing the Offset to one of its other equivalents.

The three things you will need here is a File Splitter, Hex Editor and a Anti-Virus Offset Finder. The File Splitter will cut your executable into smaller files (preferably 1 byte per file). You then use your Hex Editor on the file that holds the signature and change that signature. Or, you can keep the file complete and use your AV Offset Finder to find the Offsets automatically and just change the signatures found with your Hex Editor.

Figure 5 exhibits a script kiddie communicating signature and behavioral AV evasion strategies and mechanisms to the wider Hackforums community.

The vast majority of AI solutions are based on signatures, heuristics, and behavioral analysis. Signatures and heuristics require the creation of a specific identifier, which attackers can easily evade by mutating their malware. Behavioral analysis depends upon allowing the malware to execute in order to pre-determine its functionality, and then on assuming that it always functions in the same way. Some firms emulate an artificial environment or rely on a virtual sandbox to conduct static and dynamic analyses. These methodologies, while valid, waste resources and are imprecise because they assume that neither the malware nor its behavior will mutate [6]. One of the main, obvious problems with signature and heuristic based security solutions is that there must be an initial victim to report the malicious activity before any form of detection or prevention can occur. For some sectors, that defense is acceptable, though not ideal. For instance, the chances of jeopardizing the national security of the United States by infecting one home user, is miniscule. In contrast, a singular critical infrastructure breach, such as the 2015 breach of the Office of Personnel Management, is a cyber-Pearl Harbor against the United States and can lead to decades of cascading impacts and incidents. Most vendor AI solutions would not have prevented OPM, and many which require internet cloud connectivity, are not capable of protecting sensitive air-gapped critical infrastructure systems. Critical infrastructure organizations already struggle to efficiently allocate their limited resources without suffering the costs associated with mitigating the impacts of exfiltrated data (litigation, consumer protections, fines, etc.). Further, a detection window of two-thirds of a year makes exact forensic analysis difficult and absolute attribution impossible.

Conclusion

Reactions to cyber threats based on what has already been observed, has been experienced, or is known, are limited by the victim organization's preservation of indicators of compromise, threat information sharing culture, amount of "human error", reaction time, etc. Even after discovering a threat, it can take weeks to develop a detection signature and to disseminate it to throughout relevant sectors [1]. A sophisticated, targeted advanced persistent threat could have already laterally compromised vital systems or partner organizations in the meantime. After the signature is developed, the attacker needs only to slightly mutate their malware to continue breaching high-profile targets in the sector and exfiltrating sensitive PII, PHI, financial data, and other information. The data will be weaponized against federal agencies, public institutions, private businesses, or against the public. Critical infrastructure cybersecurity must rely on predictive, preventative, and protective solutions that detect and mitigate threats pre-execution. Organizations need machine learning AI endpoint security solutions capable of preempting and mitigating known and unknown malicious files and code based on characteristics, rather than signatures or behavior, and that are capable of scaling to protect vital systems. AI solutions can also be used to eliminate some of the exhausting manual processes and to reduce wasteful investments in antiquated technologies (such as sandboxing,

blacklisting, system isolation, detect and response tools, etc.). Further, characteristic based AI can be used to detect and prevent authentication attacks, where an adversary attempts to brute-force access to a data resource or sensitive system. It also can be used to monitor network traffic and it can be used to detect applications that are scanning for network vulnerabilities [7]. Bleeding-edge defense-grade AI solutions enable critical infrastructure owners and operators to better secure their networks, to efficiently provide their services, and to collectively protect American national security.

ICIT Contact Information

Phone: 202-600-7250 Ext 101

E-mail: <http://icitech.org/contactus/>

ICIT Websites & Social Media



www.icitech.org



<https://twitter.com/ICITorg>



<https://www.linkedin.com/company/institute-for-critical-infrastructure-technology-icit->



<https://www.facebook.com/ICITorg>

Sources

- [1] "The intelligent choice for Cybersecurity," in Cylance, 2017. [Online]. Available: <https://blog.cylance.com/the-intelligent-choice-for-cybersecurity>. Accessed: Feb. 3, 2017.
- [2] S.-A. Kristoffersen, "Artificial intelligence powered malware - A smart virus," 2016. [Online]. Available: <http://www.slideshare.net/StigArneKristoffersen/artificial-intelligence-powered-malware-a-smart-virus>. Accessed: Feb. 4, 2017.
- [3] J. Pan and C. C. Fung, "Artificial Intelligence in Malware - Cop or Culprit?," in *Research Gate*, 2008. [Online]. Available: https://www.researchgate.net/publication/268180695_Artificial_Intelligence_in_Malware_-_Cop_or_Culprit. Accessed: Feb. 4, 2017.
- [4] A. Malanov, "Securelist – information about viruses, hackers and Spam," 2016. [Online]. Available: <https://securelist.com/blog/opinions/76351/five-myths-about-machine-learning-in-cybersecurity/>. Accessed: Feb. 3, 2017.
- [5] V. Harrison and J. Pagliery, "Nearly 1 million new malware threats released every day," in *CNN*, CNN, 2015. [Online]. Available: <http://money.cnn.com/2015/04/14/technology/security/cyber-attack-hacks-security/>. Accessed: Feb. 3, 2017.
- [6] "Don't test a bomb with a hammer," in Cylance, 2017. [Online]. Available: <https://blog.cylance.com/dont-test-a-bomb-with-a-hammer>. Accessed: Feb. 4, 2017.
- [7] "How artificial intelligence is changing the face of cyber security," in *Hong Kong Business*, Hongkong Business, 2016. [Online]. Available: <http://hongkongbusiness.hk/information-technology/more-news/how-artificial-intelligence-changing-face-cyber-security>. Accessed: Feb. 3, 2017.