INTEZER

THE UNTAPPED POTENTIAL OF MALWARE CLASSIFICATION

I.THE UNTAPPED POTENTIAL OF MALWARE CLASSIFICATION

Despite the rapid pace of technology in general, few industries today are as dynamic as that of cyber security. Attackers' techniques are constantly evolving, and along with them, the potential threat.

For security teams, the challenge remains not to keep up, but rather, to outpace them. It is a persistent struggle: a never ending, record-setting marathon at a constant sprint. Even as security professionals rest, attackers are hard at work the tools and approaches used must also adapt in order to stay a step ahead in defending their organizations. Malware classification, which encompasses both the identification and attribution of code, has the power to unlock many clues that aid security teams in achieving this.

Such clues provide a greater understanding of potential adversaries. Going beyond whether code is trustworthy or malicious offers a multifaceted view into attackers' mindsets and ultimately, their goals.

Yet many security teams stop their line of inquiry once they reach a conclusion about a given file. If the code is trustworthy, no action is required. If the code is malicious, it needs to be mitigated and eradicated as quickly as possible, with recovery of important files occurring in tandem.

▶ Case closed...or is it?

Terminating a process and deleting a file offers zero guarantees and solves no problems in the long term, unfortunately. Today, it's critical (and until now, quite complicated) to both analyze threats as well as fully understand them after the initial breach. This is the one way that attackers can be remotely 'interrogated,' enabling enabling security teams to uncover the reasons behind their actions simply rather than remediating and remaining oblivious.

In analyzing any threat, teams must put themselves in the role of the attacker in order to better understand their goals and the methods they're likely to use to attain them. This involves understanding:

1 **The capabilities of the malware used.** An attacker that's eager to get a hold of sensitive internal data is going to approach an attack differently than one that aims to commit bank fraud at a financial institution. Knowing what has been compromised is only part of the critical puzzle; understanding the motive behind the attack gives organizations a clear advantage. Naturally, the use of ransomware versus adware or Trojan viruses indicates divergent malicious intentions.

2 **The type of adversary they're up against.** The power, motivation, and reach of modern criminal organizations or state-sponsored attackers differs greatly from that of an individual. Similarly, a recognizable campaign (or one that simulates existing campaigns) affects a team's immediate response, as well as the approach to safeguarding systems moving forward. When security teams have an attack profile of their potential adversary, they're better poised to remain protected, rather than only ensuring immunity from one type of attack.

3 **The attack vector.** Investigating the kill chain provides details into how an adversary (regardless of their background) will likely launch its next assault on an organization.

If a talented hacking group decides to penetrate an organization, the fact that malware has been detected and removed in one instance will not prevent future attempts. The next time the malware appears, it may likely be a more sophisticated version with stealthier methods. By only treating the 'symptom,' an organization misses out on the opportunity to comprehend its current security status. Beyond that, it remains vulnerable to the ongoing threat and spread of the 'disease'.

II. KNOWLEDGE = POWER + SECURITY

Classification Reveals Attackers' Achilles Heel

More than any other cyber security effort, classification positions security teams to be fully aware of what they're up against.

When organizations are informed, they remove the element of surprise, putting would-be attackers on the offensive. Suddenly, what would have been a lucrative breach on the attackers' side has now become more than a major operational headache, as potential adversaries are forced to alter their methods—exhausting valuable resources of their own in the process.

Until today, most cyber solutions focused on detecting threats which involved testing them in a sandbox environment or running antivirus checks. The approach has been laborious, and often, misdirected, as this method routinely overlooked malicious source code. This has indirectly led to what security industry experts have widely referred to as the *Attribution Problem;* the idea that identifying the source of a cyber attack or crime is often far too complicated and prone to mistakes because no physical evidence can be observed, and sophisticated attackers can use digital tools to extensively cover their tracks.

Classification and attribution is now easier than ever, as organizations have a powerful new tool to aid in their efforts. Led by a team of cyber security experts, Intezer has developed its novel Code Intelligence™ technology based on detecting and analyzing code reuse on a microscopic level. Its 'DNA mapping' technology enables the rapid analysis and identification of the origins of code fragments.

> *"Software is evolutionary, and just like legitimate vendors, malware authors reuse code all the time. We see code as the software's DNA, and created a massive, constantly growing database that contains both trusted and malicious DNA of software. Identifying code reuse on such a large scale enables us to detect completely new malware, as well as automatically classifying it to the precise family. Diving into the code brings a microscopic level of detail and creates new possibilities for malware analysis and detection."*
>
> Roy Halevi, CTO and Co-founder

Within seconds, a given file or binary is dissected into thousands of small fragments, and then compares them to Intezer's Genome Database, a massive, industry-first development containing billions of pieces of code ('genes') from legitimate and malicious software offering an unparalleled level of understanding of potential threats. The Genome Database is constantly growing, creating a library of knowledge for security professionals.

Using this database, Code Intelligence™ can recognize even a small portion of reused code. Security teams are capable of near-instantaneous detection and accurate, comprehensive analysis, which offers critical insight into attackers' abilities as well as their motives.

Closing the Skill Gap While Enabling Alert Prioritization ▶ ▶ ▶

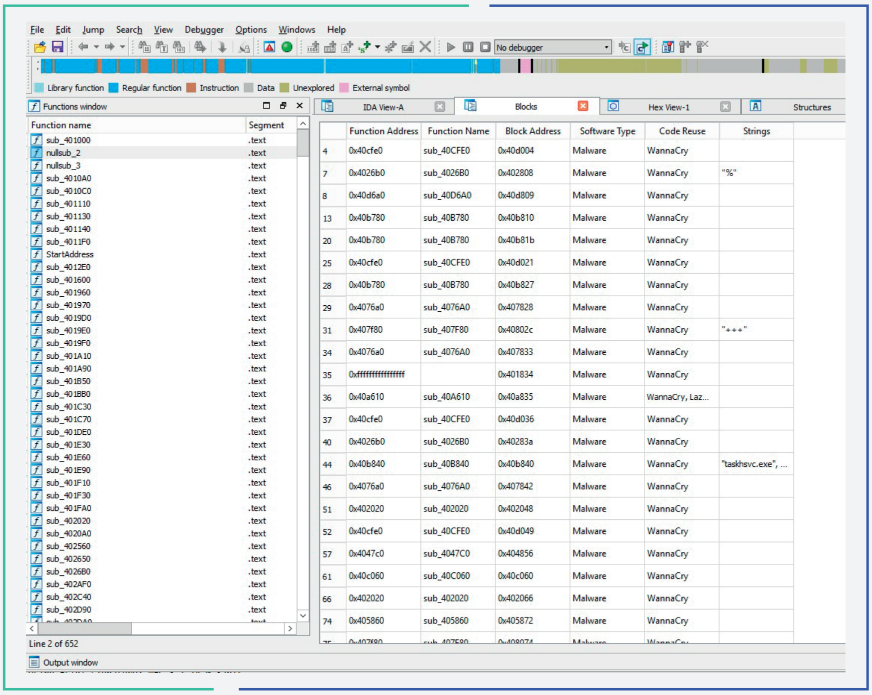
Many organizations receive hundreds (or even thousands) of alerts -including a fair number of which are false positives -which negatively impact operational efficiency. Previously, skilled reverse engineers were required to be able to manually backtrack an attacker's moves and understand the intention behind an attack.

Intezer has managed to close this critical skill gap with Intezer Analyze™, a solution that enables security professionals to filter through the hundreds (and sometimes even thousands) of alerts and reduce false positives, which can negatively impact operational efficiency.

The company has made this possible by integrating Security Identification Event Management (SIEM) or any other alert system with its API, automatically sending every file into Intezer Analyze™ to map its DNA. Intezer's Genome Database is comprised of trusted and malicious software, and as such, enables companies to recognize and accurately identify files that are either benign or problematic, as well as those that contain instances of both types.

Classifying files into threat categories also gives companies a distinct advantage: thanks to an additional layer of specificity, IR teams can effectively prioritize alerts. (A nation-sponsored attack, for example, requires immediate attention and eradication over an instance of generic malware.)

The company has made an automated version of reverse engineering possible through a special plugin Intezer has developed to IDA Pro, which generates for every code block the actual code reuse classification, saving critical time during this stage and improving the speed with which teams respond to relevant threats.



Function name	Segment
sub_401000	.text
nullsub_2	.text
nullsub_3	.text
sub_4010A0	.text
sub_4010C0	.text
sub_401110	.text
sub_401130	.text
sub_401140	.text
sub_4011F0	.text
StartAddress	.text
sub_4012E0	.text
sub_401600	.text
sub_401960	.text
sub_401970	.text
sub_4019D0	.text
sub_4019E0	.text
sub_4019F0	.text
sub_401A10	.text
sub_401A90	.text
sub_401B50	.text
sub_401BB0	.text
sub_401C30	.text
sub_401C70	.text
sub_401DE0	.text
sub_401E30	.text
sub_401E60	.text
sub_401E90	.text
sub_401F10	.text
sub_401F30	.text
sub_401FA0	.text
sub_402020	.text
sub_4020A0	.text
sub_402560	.text
sub_402650	.text
sub_4026B0	.text
sub_402AF0	.text
sub_402C40	.text
sub_402D90	.text

Line 2 of 652

	Function Address	Function Name	Block Address	Software Type	Code Reuse	Strings
4	0x40cfe0	sub_40CFE0	0x40d004	Malware	WannaCry	
7	0x4026b0	sub_4026B0	0x402808	Malware	WannaCry	"%"
8	0x40d6a0	sub_40D6A0	0x40d809	Malware	WannaCry	
13	0x40b780	sub_40B780	0x40b810	Malware	WannaCry	
20	0x40b780	sub_40B780	0x40b81b	Malware	WannaCry	
25	0x40cfe0	sub_40CFE0	0x40d021	Malware	WannaCry	
28	0x40b780	sub_40B780	0x40b827	Malware	WannaCry	
29	0x4076a0	sub_4076A0	0x407828	Malware	WannaCry	
31	0x407f80	sub_407F80	0x40802c	Malware	WannaCry	"+++"
34	0x4076a0	sub_4076A0	0x407833	Malware	WannaCry	
35	0xffffffffffffffff		0x401834	Malware	WannaCry	
36	0x40a610	sub_40A610	0x40a835	Malware	WannaCry, Laz...	
37	0x40cfe0	sub_40CFE0	0x40d036	Malware	WannaCry	
40	0x4026b0	sub_4026B0	0x40283a	Malware	WannaCry	
44	0x40b840	sub_40B840	0x40b840	Malware	WannaCry	"taskhsvc.exe", ...
46	0x4076a0	sub_4076A0	0x407842	Malware	WannaCry	
51	0x402020	sub_402020	0x402048	Malware	WannaCry	
52	0x40cfe0	sub_40CFE0	0x40d049	Malware	WannaCry	
57	0x4047c0	sub_4047C0	0x404856	Malware	WannaCry	
61	0x40c060	sub_40C060	0x40c060	Malware	WannaCry	
66	0x402020	sub_402020	0x402066	Malware	WannaCry	
74	0x405860	sub_405860	0x405872	Malware	WannaCry	

III. BUILDING ORGANIZATIONS' IMMUNITY

From an operations perspective, Intezer Analyze™ offers an easy integration with internal security processes, including automation and forensics tools. When testing code, it is possible to know with confidence in just a few seconds if it stems from a trusted or malicious source. Any files flagged as malicious (detailing specific malware families and related campaigns) can be further scrutinized by internal teams in order to anticipate threat capabilities, the attacker's specific goal, and their identity or known affiliations.

As explained in *our blog,* if malware possessing genes from Mimikatz has been detected, it implies that *this adversary will at some point attempt to undertake a lateral movement within your network,* seeking the ability to then spread to other computers with greater permissions and access points.

Recommendations made by security teams in this stage have both the potential for improved future response and a direct impact on future security.

Intezer's technology uncovered *the link between WannaCry and the alleged North Korean threat actor, Lazarus,* which enabled customers to immediately detect this emergent type of malware and know that it is related to a nation-sponsored attacker—to prioritize their mitigation efforts accordingly.

Similarly, Intezer has empowered its users to create 'antidotes' (e.g. remediation in different formats, such as YARA signatures, OpenIOC, or STIX, among others) for installation on their existing security solutions that encompass the entire Lazarus code base. As a result, they can 'vaccinate' against an adversary, not only a specific attack. Simply put, this means that the enemy must start at square one, which requires an enormous amount of time, money and patience. For organizations, there is no stronger position than bolstering defenses while impeding attackers' processes.

Interested in taking your team's detection and analysis process to the DNA level?

Contact Intezer's expert team to learn more about how we can help.