Family Ties: Multigenerational Ransomware Family Analysis Using Intezer

Author: Justin Harris, justin.r.harris@hotmail.com
Advisor: *David Hoelzer*

Accepted: *December 15, 2022*

Abstract

The adoption of the Ransomware as a Service (RaaS) model has rapidly evolved the ransomware threat landscape. As a result, ransomware binary analysis of next-generation samples contains marginal code similarities with early generations within the same family. Often new generations of ransomware detection incorrectly identify the ransomware family. Infrastructure, tools, techniques, and procedures (TTPs), or ransom notes often determine the initial ransomware classification. Code similarities could assist investigators in identifying RaaS groups working on multiple ransomware families. Identifying common coding tactics in highly developed code allows security researchers to expedite attribution and develop mitigation strategies. Law enforcement can use code similarity analysis to show affiliation between ransomware groups. This paper aims to determine whether code similarities exist between next-generation ransomware and early-generation binaries. Research focuses on ransomware families containing four generations and analyzes randomly selected binaries using an automated genetic tool. Intezer's genetic analysis compares binary samples against Intezer's malware code repository. Intezer allows incident responders to analyze ransomware binaries and identify malware more accurately and quickly.

1. Introduction

The prominence of ransomware attacks has been increasing over the past several years. The ransomware attack impact has also been increasing. Nearly 53% of ransomware victims have noticed an increase in impact in the previous year (Sophos, 2022). The Darkside ransomware attack against Colonial Pipeline in May 2021 caused gas shortages for thousands of Americans (Marks & Schaffer, 2022). The United States government initiated a whole-of-government approach to handling the Colonial Pipeline intrusion (The White House, 2021). The increased attention persuaded Darkside to rebrand its ransomware operations.

The RaaS model has allowed ransomware groups like Darkside to adapt to defensive countermeasures and law enforcement retaliation quickly. Ransomware groups can change ransomware source code and infrastructure in a short amount of time. This rapid change can cause investigators to struggle to correctly attribute new ransomware attacks to individual ransomware families. An in-depth analysis of ransomware binaries can reveal patterns that signify relationships between ransomware families (Dudley & Golden, 2022, p. 205). Patterns like code reuse can indicate ransomware developers working for multiple ransomware families (Rosenberg, 2021). Online tools such as Intezer perform a comparative analysis between binaries to help identify common "genes." These “genes” are small pieces of extracted code from each submitted binary (Fridman, 2018).

Symantec analysis suggested members of the Darkside ransomware groups have evolved into several new ransomwares. The Darkside successors include BlackMatter, BlackCat, ALPHV, and Noberus (Symantec, 2022). These ransomware variants are members of the same ransomware family. Ransomware families are code samples that share most of their code with other samples (Boczan & Williams, 2020).

This research focuses on the code analysis between generations of ransomware within a given family. Intezer analyzes the uploaded ransomware samples. The online tool, Intezer, is an automated analysis tool that breaks code into segments called genes (Fridman, 2018). These genes represent code similarities between other malware from Intezer’s database. As a ransomware family's lineage expands, the ratio of genes between

generations may significantly decrease. Furthermore, ransomware binaries may exhibit genes relating to one or more malware families. These interrelated malware families could indicate that RaaS developers or individual developers work for multiple groups.

2. Research Method

The research begins with obtaining binary files for analysis. Ransomware binary repositories, such as MalwareBazaar, provide simple solutions to obtaining these binary files. MalwareBazaar allows users to search for tags related to the binary files of interest. For example, searching MalwareBazaar's database for "tag:nefilim" returns Nefilim ransomware samples. VirusTotal is a secondary malware repository that allows custom searches for binary samples. MalwareBazaar and VirusTotal were used to download ransomware binaries.

The ransomware binaries are uploaded to Intezer after being downloaded from online repositories. Intezer allows users to create free accounts with 14 days of free Enterprise access. An Intezer's Enterprise access account conducted the binary analysis. Intezer's analysis provides a genetic summary and the related samples of each malware binary. The related samples section provides the “Related Families” information along with the corresponding number of genes. Then the genetic summary results from Intezer’s static and dynamic analysis are displayed. Additionally, a hybrid analysis was performed on each ransomware binary.

2.1. What are Ransomware Families?

Ransomware families are code samples that share most of their code with other samples. However, ransomware families are often classified by their collection of Tools, Tactics, and Procedures (TTPs). Each ransomware family operates with very similar fundamental procedures leading to the encryption of victim data. Then the ransomware drops a ransom note with the demands and ransom amount on the victim's computer. Investigators often rely on data in these notes to determine the ransomware family (Bitdefender Enterprise, 2022). This research focuses on ransomware code analysis using Intezer to analyze the code segments.

2.2. What is Binary Code Analysis?

Binary code analysis can be performed dynamically, statically, or symbolically. Intezer analysis focuses on dynamic and static analysis methods. Dynamic analysis observes and monitors the binary file while executing (Qasem et al., 2022, p. 25:7). Dynamic analysis is often called behavioral analysis due to monitoring the binary file's behavior upon execution. Static analysis does not rely on binary file execution. Instead, it examines the code of the binary files. Static analysis tools attempt to examine the non-running code of the binary file (Dewhurst, 2022).

2.3. What is the Intezer Analysis Tool?

Intezer is a free online automation tool with options for commercial licenses. The automated analysis breaks the code into blocks called genes. Intezer compares the binary genes against their malware genome database, and the cross-comparison identifies genes related to other known malicious binaries. Additionally, the genetic summary will identify segments related to administrative tools, code packers, unique code, and common code. Figure 1 shows a binary analysis example for a DarkSide ransomware binary. The genetic analysis includes the Genetic Summary, Related Samples, Code, Strings, and Capabilities categories produced by Intezer's analysis. This research focuses mainly on the Genetic Summary and Related Samples sections of Intezers analysis.

Figure 1. Intezer Analysis Example

3. Findings and Discussion

Binary analysis is performed on the ransomware binaries for the Nefilim, Darkside, and Chaos families. Each family has at least four ransomware associated with the family, and each binary was analyzed using the automated tool, Intezer. Binary research focuses on the genetic summary of each generation within a malware family. The percentage of shared genes may not equal 100% due to genes shared by multiple malware families (Intezer, n.d.).

3.1. Nefilim Family

Nefilim Ransomware is a double extortion ransomware that first appeared in the wild in March 2020. Double-extortion ransomware exfiltrates victim data from compromised systems before encrypting the data. The exfiltrated data is exposed on a website if the ransom demands still need to be met. Nefilim evolved from two earlier versions of ransomware called Nemty (Agcaoili & Gelera, 2021) and JSWorm (Sinitsyn, 2021). JSWorm ransomware was first seen in April 2019, and Nemty was first seen in August 2019. In late 2021, Nefilim evolved again to become Karma ransomware (Toulas, 2021). Karma was the latest evolution of Nefilim. The Nefilim family consists of four primary generations: JSWorm, Nemty, Nefilim, and Karma ransomware.

3.1.1. JSWorm Ransomware

JSWorm ransomware is the first in the Nefilim family's lineage. Three ransomware binaries were randomly sourced from VirusTotal. Figure 2 lists the JSWorm binary samples used for the first generation of the Nefilim ransomware family analysis.

No.	Ransomware	SHA1 Hash	Source
1	JSWorm	7388a0b44b15dc57e552395a2de36f433a47cc37	VirusTotal
2	JSWorm	afc25f8f3bd300ea70c0e68358588df85950fdd9	VirusTotal
3	JSWorm	7600f09f914830fa6054defdb97a8d70ce6036ef	VirusTotal

Figure 2. JSWorm Binary Metadata

JSWorm No. 1 was identified as malicious; however, Intezer did not categorize it as JSWorm Ransomware. The malware binary was identified as malicious software. Over 48% of the code was unique. More than 35% of the code is related to administrative tools

such as KeyMagic, TeamViewer GmbH, and AdFind. The JSWorm No. 1 binary utilized code or functions from previously existing tools.

Intezer identified JSWorm No. 2 binary as malicious and did not categorize the binary as JSWorm ransomware. Approximately 60% of JSWorm No. 2 code was unique. Over 10% of JSWorm No.2 shared code with the administrative tools TeamViewer GmbH and KeyMagic. However, JSWorm No. 2 shared code with two other ransomware families named MonaLisa ransomware and Clown ransomware. JuicyPotato is a privilege escalation tool used in a Windows environment (Fortinet, n.d.).

MonaLisa ransomware, DMR ransomware, and JuicyPotato code were present in the JSWorm No. 3 sample. The third JSWorm sample shares 11% of its code with TeamViewer GmbH and KeyMagic. Over 65% of the JSWorm No. 3 code is unique. All three JSWorm binaries have reused code from other known ransomware families. However, most of JSWorm's code reuse is from administrative tools, or the code is unique to the binary sample. Figure 3 illustrates the genetic breakdown of each ransomware sample and the corresponding percentage of related code.

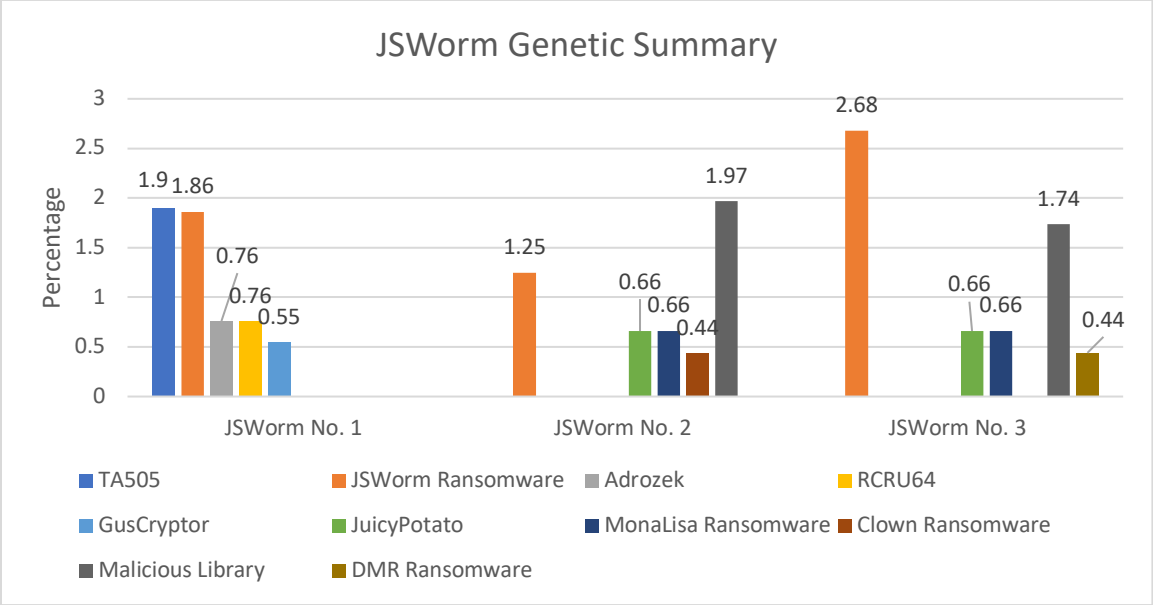

Figure 3. JSWorm Genetic Summary

3.1.2. Nemty Ransomware

Nemty is the second generation of ransomware in the Nefilim family. Nemty ransomware first appeared in August 2019. Two actors named, Jingo and JSWorm, were seen recruiting affiliates with a 70/30 profit split (Fuentes et al., n.d., p. 13). RaaS groups divide operations into operators and affiliates. Profit sharing between operators and affiliates is determined when affiliates are recruited (Baker, 2022).

Three Nemty binaries were downloaded from MalwareBazaar. Figure 4 lists the Nemty binary metadata.

No.	Ransomware	SHA1 Hash	Source
1	Nemty	7c120db30a9ef055c0d41ab5efeaaf93dce5742e	Malware Bazaar
2	Nemty	838bb61c5db51ff145e436cd04bea3af018b8478	Malware Bazaar
3	Nemty	aab76fefd4ebf7408a4224e3d38873f605ef4ed4	Malware Bazaar

Figure 4. Nemty Binary Metadata

The Nemty No. 1 and Nemty No. 2 binary files had similar results. Nemty No. 1 had 15 code genes related to Nemty's successor, Nefilim ransomware. Approximately 77% of the Nemty No. 1 code related to Nefilim, and 22% of the code was identified as malicious libraries. Nemty No. 2 had 16 code genes, and approximately 78% of the code was unique to Nefilim ransomware. The high percentage of Nefilim-related code could indicate that Nefilim ransomware heavily relied on Nemty's source code.

Intezer did not identify Nemty No. 3 code relating to any generation of the Nefilim family. However, Nemty No. 3 code genes relate to DanaBot and STOP ransomware. Nemty ransomware may have used DanaBot's credential-stealing functionality to obtain credentials to exploit a victim further. DanaBot is a credential-stealing malware that became popular in 2018 (Trend Micro, 2018). STOP Ransomware was first seen in 2019, around the same time Nemty ransomware was first released (Trend Micro, 2019). More than 67% of Nemty No. 3 ransomware was unique code.

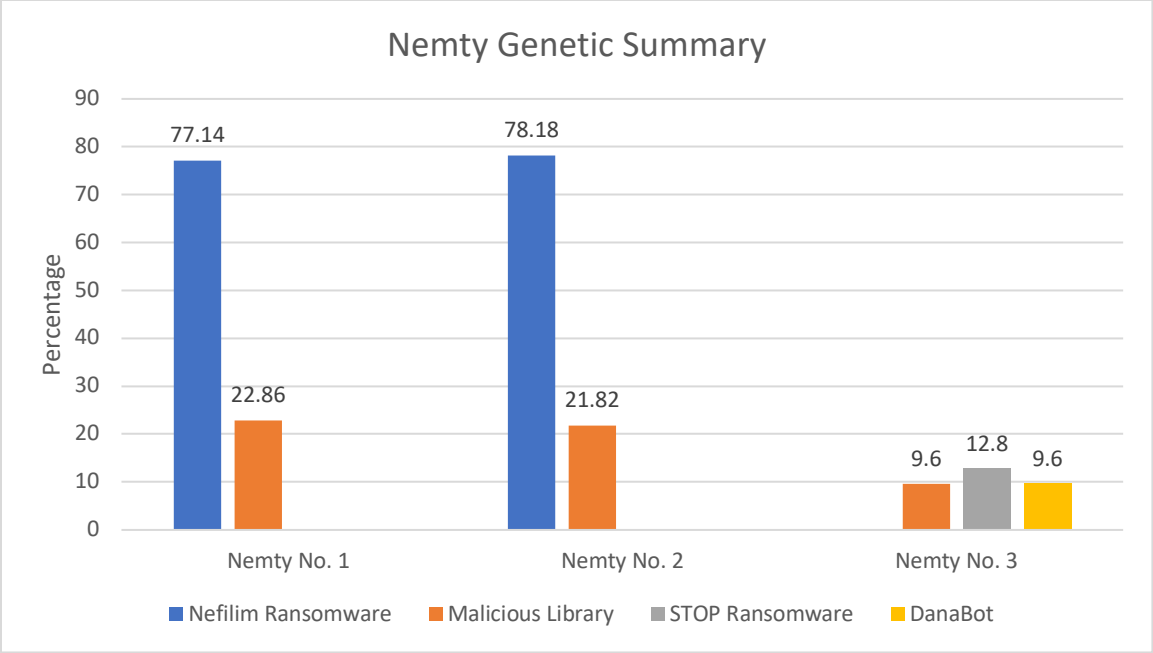

Figure 5. Nemty Genetic Summary

3.1.3. Nefilim Ransomware

Nefilim is the third and most impactful generation of the Nefilim ransomware. Nefilim focused on data extortion and operated under the RaaS model. The ransomware did not focus on a particular industry (Tancio, 2022). Instead, Nefilim actors targeted large companies with substantial revenue. The ransom demands were proportionate to the company's publicly reported annual revenue. The initial intrusion vector was shared among several ransomware organizations. Nefilim's success was the most prolific generation in the Nefilim family.

The ransomware binaries were randomly selected from MalwareBazaar. Figure 6 lists the Nefilim binary metadata analyzed by Intezer.

No.	Ransomware	SHA1 Hash	Source
1	Nefilim	2a044e5e3dde62ded6a3f2a5a634067168a41810	Malware Bazaar
2	Nefilim	c735ff582ab489f13cfc76ee744e52b868012e2e	Malware Bazaar
3	Nefilim	802a5fc4f1fdfae4a8cf99a4544c191641f9bceb	Malware Bazaar

Figure 6. Nefilim Binary Metadata

The Nefilim analysis results are unique compared to the previous two Nefilim generations. Intezer identified that most of the code for the first two binary files contained 92% of Nefilim's code. The third generation has the purest results relating directly to itself. The first and second Nefilim family generations contained code relating to siblings or non-Nefilim malware.

The third binary contained 70.48% of Nefilim's code. The Nefilim No. 3 contained no code relating to previous generations in the Nefilim ransomware family. Nearly 10% of the Nefilim No. 3 ransomware sample consisted of malicious code libraries. The third generation of the Nefilim family appears to redesign the ransomware code with minimal code reuse from earlier generations.

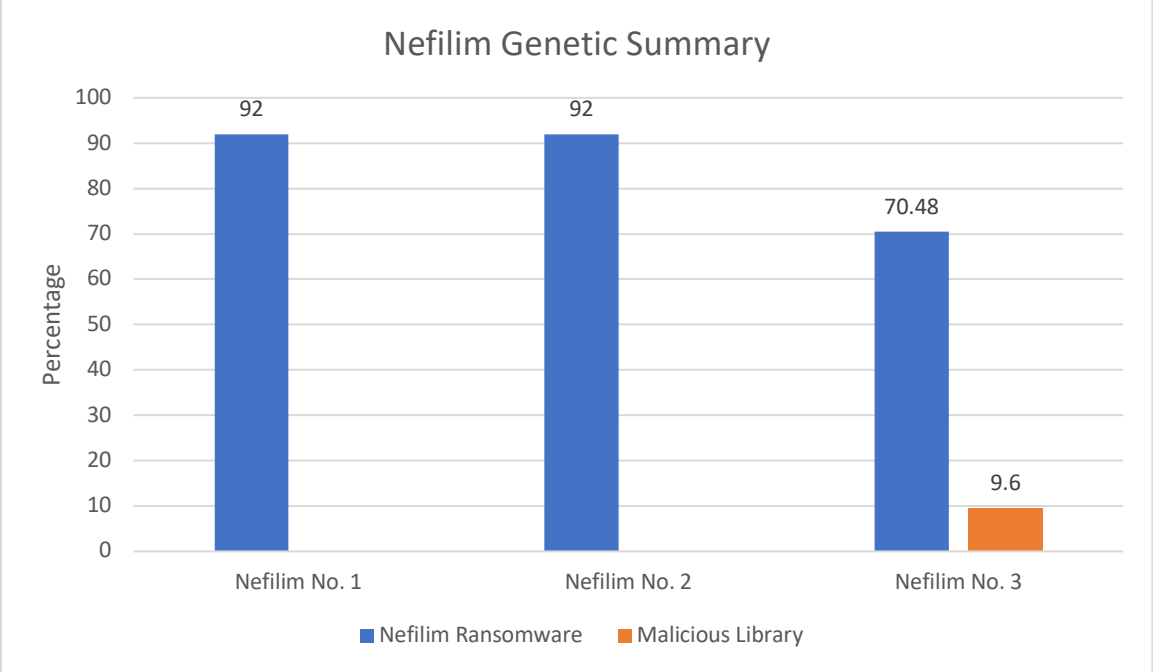

Figure 7. Nefilim Genetic Summary

3.1.4. Karma Ransomware

Karma is the most recent generation of ransomware in the Nefilim ransomware family. Karma ransomware first appeared in June 2021 and targeted companies similar to Nefilim ransomware (Terefos, 2021). Ransomware was seen in 2016 with the same name, Karma (Abrams, 2016). The fourth generation in the Nefilim family is not a descendant of the 2016 version of Karma ransomware.

Three Karma binary files were randomly sourced from Malware Bazaar. Figure 8 includes the ransomware binary metadata.

No.	Ransomware	SHA1 Hash	Source
1	Karma	08f1ef785d59b4822811efbc06a94df16b72fea3	Malware Bazaar
2	Karma	5ff1cd5b07e6c78ed7311b9c43ffaa589208c60b	Malware Bazaar
3	Karma	9393c82779388b2a27686506e3d845f73ecc93bd	Malware Bazaar

Figure 8. Karma Binary Metadata

Karma No. 1 is the first generation to contain code genes relating to multiple Nefilim family ransomware. All the Karma binaries share over 11% of code related to JSWorm and Nefilim ransomware. The genetic summary indicates that the Karma No. 1 and Karma No. 2 binaries are comprised of 92.61% Karma ransomware code.

The third Karma binary contains 78.01% of Karma's unique code. Intezer's analysis implies Karma developers reused small amounts of the early Nefilim generation family. Karma No. 3 used slightly less Nefilim and JSWorm code than Karma No. 1 and Karma No. 2 binaries. While Karma is the first generation to have relationships with multiple Nefilim generations, the related code is marginal between ancestors.

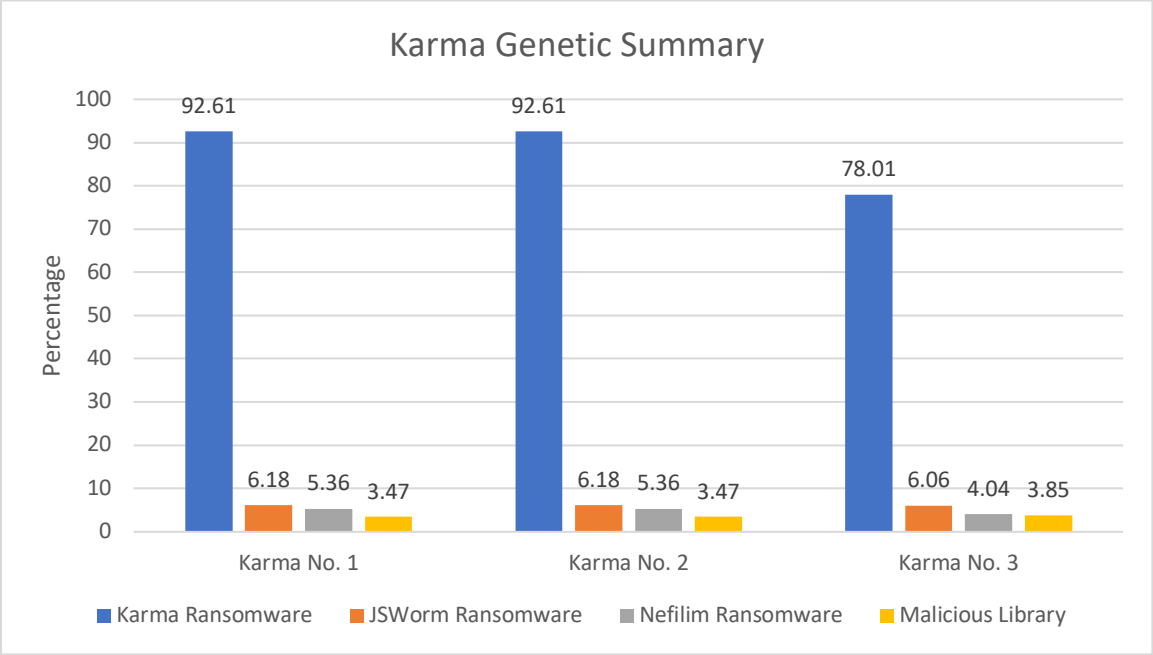

Figure 9. Karma Genetic Summary

Justin Harris, justin.r.harris@hotmail.com

3.2. Darkside Family

The Darkside family gained prominence after the Colonial Pipeline attack in May 2021. However, Darkside first emerged in August 2020. The Darkside side family follows the Ransomware as a Service model and applies multiple extortion techniques to its victims. Shortly after Darkside announced it was shutting down servers, a new ransomware named BlackMatter appeared. BlackMatter is a rebrand and second generation of Darkside ransomware. Like Darkside, law enforcement pressure caused BlackMatter to disband quickly in October 2021.

BlackCat is the third generation in the Darkside family. Unlike BlackCat's predecessors, this ransomware was written in the Rust language. The adoption of the Rust language can cause difficulty in analysis and detection (Microsoft Defender Threat Intelligence, 2022). BlackCat first appeared in November 2021.

Two additional ransomware named ALPHV and Noberus are synonymous with BlackCat ransomware. ALPHV and Noberus used the cross-platform language Rust, and both ransomware first appeared in November 2021. The ransomware appears to be modified versions within the same generation as BlackCat. However, operational variances suggest different affiliate groups are operating each ransomware.

In summary, the DarkSide ransomware family has direct lineage with BlackMatter, BlackCat, and Noberus ransomware.

3.2.1. Darkside Ransomware

Darkside ransomware peaked in February 2021 while infecting more than 20 victims (Nuce et al., 2021). The Colonial Pipeline attack gained international law enforcement attention. The increased attention led the United States Department of State to issue a $10 million reward for information leading to the identification of the individuals responsible for the pipeline attack (U.S. Department of State, 2021). Shortly after the initial attack, Darkside announced they were shutting down operations.

The Darkside ransomware binaries in Figure 10 were obtained from Malware Bazaar.

No.	Ransomware	SHA1 Hash	Source
1	Darkside	03c1f7458f3983c03a0f8124a01891242c3cc5df	Malware Bazaar
2	Darkside	7e01305dd52b6c92d97e88c870410381577cad61	Malware Bazaar
3	Darkside	dfc4f8f01c18e8b9979ea1d5f67a2165a9de1e5d	Malware Bazaar

Figure 10. Darkside Binary Metadata

Darkside No. 1 had a genetic structure identified as 83.56% Darkside ransomware. Only 1.05% of the code relates to BlackMatter ransomware. The relationship to a future generation of Darkside is likely due to reuse in BlackMatter. The second Darkside binary was nearly 97% Darkside ransomware. A unique series of four genes related to Simda botnet malware. Simda is an older botnet with credential-harvesting capabilities (Cybersecurity & Infrastructure Security Agency, 2016). The Darkside No. 3 binary only related to malicious code belonging to BlackMatter and Darkside ransomware. All three samples used UPX packer code. The binaries were between 0.66% and 13.85% of UPX packer code.

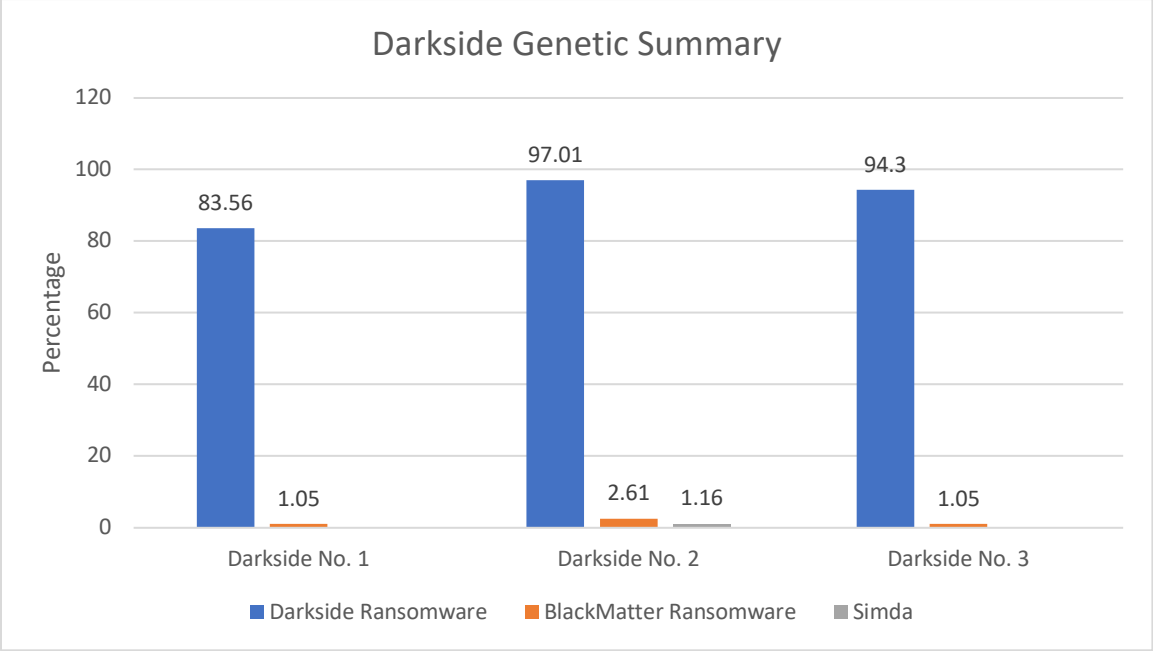

Figure 11. Darkside Genetic Summary

3.2.2. BlackMatter Ransomware

The global response and scrutiny caused Darkside actors to rebrand their ransomware. BlackMatter ransomware was the first known spawn of the Darkside group (Cybersecurity and Infrastructure Agency, 2021). After first appearing in July 2021, BlackMatter quickly announced its disbandment in October 2021. Figure 11 list the metadata for three BlackMatter binaries that Intezer analyzed.

No.	Ransomware	SHA1 Hash	Source
1	BlackMatter	80a29bd2c349a8588edf42653ed739054f9a10f5	Malware Bazaar
2	BlackMatter	721a749cbd6afcd765e07902c17d5ab949b04e4a	Malware Bazaar
3	BlackMatter	1ed39024b03b3490049b4d6f2577ca36e18b405a	Malware Bazaar

Figure 12. BlackMatter Binary Metadata

The BlackMatter No. 1 binary genetics indicated the majority of the code related to BlackMatter ransomware. Nearly 36% of the binary shared genes with LockBit ransomware, and less than 1% of the code genes belong to Darkside ransomware.

The genetic summary for BlackMatter No. 2 was similar to the first BlackMatter binary. The shared genetic code was related BlackMatter and LockBit ransomware at 86.39% and 37.87%, respectively. The second binary has Darkside-related code resulting in less than 1%. The BlackMatter No. 3 binary consisted of genes from the BlackMatter, LockBit, and Darkside. All three BlackMatter ransomware binaries contain non-malicious genes from “The Qt Company Ltd." Two of the binaries used UPX Packer code.

In summary, the BlackMatter ransomware binaries frequently reuse code from the Lockbit ransomware. The majority of the BlackMatter code is unique to itself. However, there was minimal code reuse from Darkside.

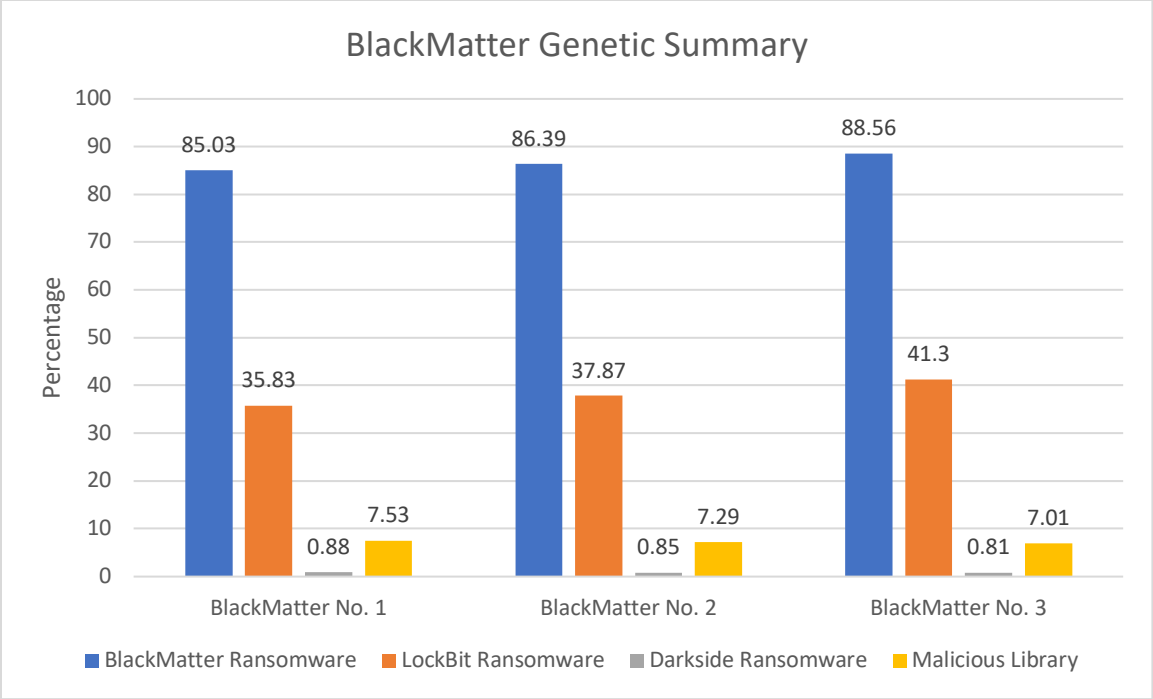

Figure 13. BlackMatter Genetic Summary

3.2.3. BlackCat/ALPHV Ransomware

BlackCat, also known as ALPHV, is ransomware with connections to Darkside. Like BlackMatter, Blackcat ransomware was generated from the fallout of Darksides' dissolution. Both ransomwares are considered within the same generation of Darksides lineage.

RaaS developers promoted the ransomware as ALPHV on forums; however, the MalwareHunterTeam named the ransomware BlackCat due to a black cat favicon on the TOR payment site (Abrams, 2021). The randomly selected binaries were identified as BlackCat in Malware Bazaar's database.

No.	Ransomware	SHA1 Hash	Source
1	BlackCat	e22436386688b5abe6780a462fd07cd12c3f3321	Malware Bazaar
2	BlackCat	20d7a428a340e30ff3f3ea5c43b4e2c1f4a1d0cb	Malware Bazaar
3	BlackCat	11331c98855fdf42bd94a84687661c682336fea9	Malware Bazaar

Figure 14. BlackCat and ALPHV Binary Metadata

BlackCat ransomware binaries do not contain code relating to sibling ransomware in the Darkside family. Instead, all three binaries consisted of Hive ransomware genes. BlackCat No. 2 contained nearly 7% of Hive ransomware code genes. Most of the BlackCat binary code was identified as BlackCat ransomware genes. The remaining malicious code genetics was malicious libraries or generic malware.

The non-malicious code category in each binary included code packers. The BlackCat developers used code from ASPack and UPX packers. The BlackCat No. 3 incorporated Tor genetic code. The BlackCat No. 2 binary contained unusual code classifications, such as Unlabeled and Microsoft Corporation. Overall, the BlackCat binaries had no code relationship to previous ransomware in Darkside. The ransomware used code from Hive and other malicious libraries.

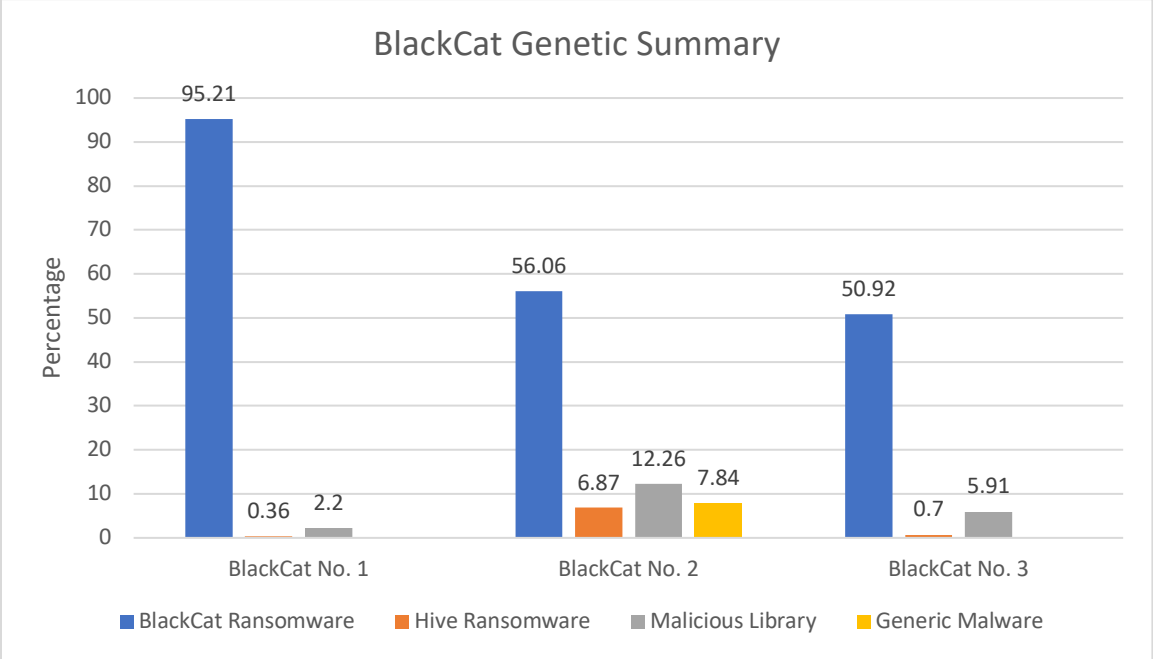

Figure 15. BlackCat Genetic Summary

3.2.4. Noberus Ransomware

Noberus is closely related to BlackCat ransomware and was first seen in November 2021. The ransomware is considered to be in the same generation as BlackCat/ALPHV. However, recent Symantec reporting indicates that Noberus developers upgraded the ransomware. Upgrades included ARM build for encryption on non-standard architectures and encryption functionality in Windows Safe Mode

(Symantec, 2022). Noberus binary analysis was completed to indicate if there was any source code from other malware families.

The Noberus binaries were identified using VirusTotal's search capabilities. The VirusTotal search parameter "symantec:Ransom.Noberus" returned 26 results. Figure 16 shows three randomly selected Noberus binary files for analysis.

No.	Ransomware	SHA1 Hash	Source
1	Noberus	396c75df80e54829d5482d290a6df00c09301fb3	VirusTotal
2	Noberus	857cc056290d5a1327a389277b1ceb5b63f4a506	VirusTotal
3	Noberus	0b0b67d9247aa18a70217a3ad5dd078b6811381e	VirusTotal

Figure 16. Noberus Binary Metadata

Intezer's genetic summary for Noberus was primarily similar to BlackCat. All three binary files were identified as BlackCat Ransomware, Hive, and Malicious Library. The first binary consisted of 51.37% of BlackCat's genetic code, whereas Noberus No. 2 and Noberus No. 3 had 95% or more BlackCat genetic code. The Hive genetic code was less than 1% in each analyzed binary.

The same packers in BlackCat ransomware, UPX, and ASPack, were seen in the Noberus samples. The Noberus results are nearly identical to BlackCat. The results reaffirm that the ransomware is within the same generation of the Darkside family.

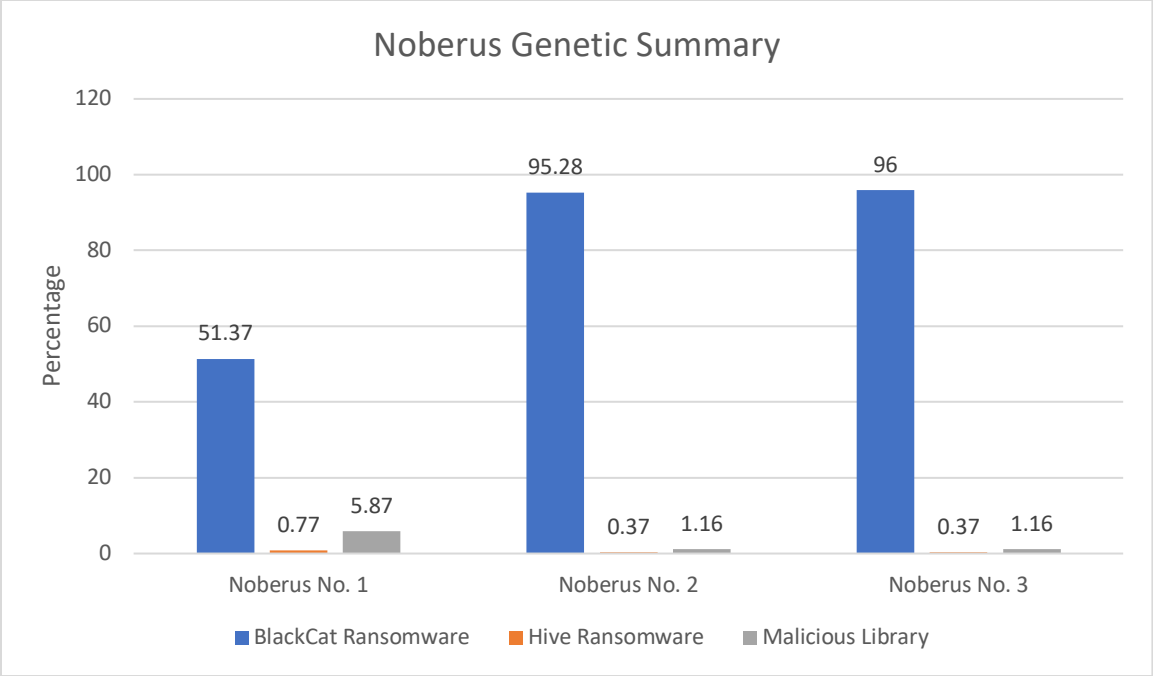

Figure 17. Noberus Genetic Summary

3.3. Chaos Family

The Chaos ransomware family originated as a ransomware builder kit. A ransomware builder kit is a closed-source customizable program provided to ransomware customers. The ransomware authors created the Chaos kit to provide criminal groups with the ability to generate a weaponized binary. The new binary is tailored to the criminal group's infrastructure (Constantin, 2022).

The first two versions of the Chaos ransomware builder lacked encryption functionality. Chaos ransomware builder version 3.0 first appeared in June 2021 and introduced encryption capabilities (Smith, 2021). Chaos version 4.0 presented the second generation in the Chaos family. The second generation is called Onyx ransomware and first appeared in April 2022. Onyx renamed itself to VSOP ransomware in August 2022 and recycled established infrastructure such as the extortion site. The most recent version of the Chaos family rebranded itself as Yashma ransomware.

3.3.1. Chaos Ransomware

The Chaos ransomware listed in Figure 18 begins with Chaos version 3.0 or higher. Chaos version 3.0 is when the malware begins to behave as ransomware. The Chaos binaries in Figure 18 were sourced from MalwareBazaar and VirusTotal.

No.	Ransomware	SHA1 Hash	Source
1	Chaos	59a80c57499b6eb5de31fcbf582eeeb1c3b20e9d	MalwareBazaar
2	Chaos	67d18715f746cc914bfffc502354547c388d7af0	VirusTotal
3	Chaos	fb813e713df734f368163214506a52dbc364c954	MalwareBazaar

Figure 18. Chaos Binary Metadata

The Chaos No. 1 binary consists of 43 Chaos ransomware code genes and 83.35% of shared Chaos code. Three code genes were unique to other known malicious libraries.

The second binary is comprised of nearly 81% generic malware code. However, the Chaos No. 2 binary had 44.94% matching Chaos ransomware code. These results are significantly less than the first Chaos binary results. The second binary analysis resulted in 5.66% of the code matching SolidBit ransomware. The SolidBit ransomware is loosely related to the Yashma builder according to online marketing of the affiliate programs (Hill, 2022).

The third Chaos binary that Intezer analyzed was very similar to the second Chaos binary. The vast majority of the genetic code was identified as generic malware. The Chaos ransomware genetic code equaled 43.32%, with the code genes equaling 31. The most exciting data was that 7.25% of the genetic code belonged to SolidBit, and 1.19% belonged to Yashma ransomware. The Chaos No. 3 binary shows a relationship between SolidBit ransomware and Yashma ransomware. These findings support SolidBit RaaS online statements that they rebranded Yashma ransomware. However, the code analysis indicates that the overlap is negligible.

The first and second Chaos binaries consisted of non-malicious code such as UPX Packer and unique codes. Chaos No. 1 was only binary without an administrative code identified. In summary, Intezer's analysis revealed minor code similarities between first-generation Chaos ransomware and the more recent Yashma ransomware.

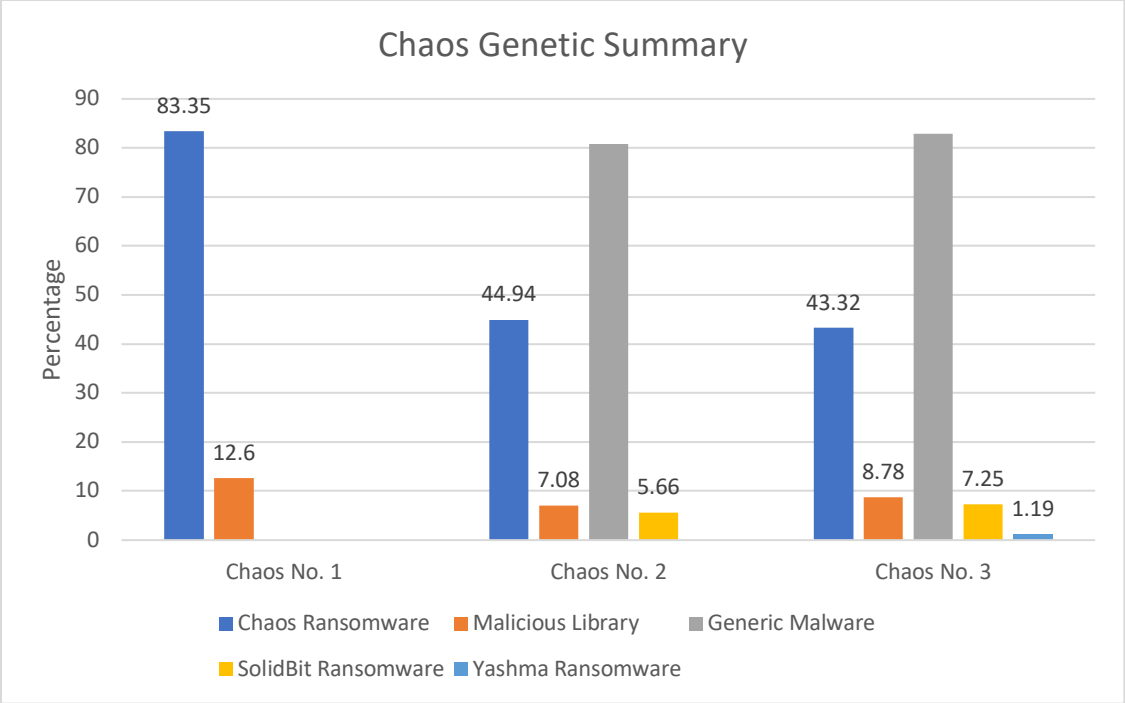

Figure 19. Chaos Genetic Summary

3.3.2. Onyx Ransomware

Onyx ransomware first appeared near the end of April 2022. The ransomware overwrites files that are larger than 2 MBs (Dunn, 2022). The overwriting function is similar to the early Chaos ransomware builder version. The ransomware used double extortion to encourage victims to pay the ransom. Due to Onyx's short life cycle and lack of victim reporting, research only discovered one Onyx binary file. MalwareBazaar database searches for "Onyx" resulted in an earlier version of ransomware called OnyxLocker. There was only one positive search result for Onyx ransomware relating to the April 2022 ransomware. Open-source research suggests no relationship exists between Onyx and OnyxLocker (Hall, 2019). Figure 20 represents the metadata for the 2022 Onyx ransomware malware analyzed by Intezer.

No.	Ransomware	SHA1 Hash	Source
1	Onyx	a4f5cb11b9340f80a89022131fb525b888aa8bc6	MalwareBazaar

Figure 20. Onyx Binary Metadata

Onyx No. 1 analysis begins with 79.64% of the genetic code relating to Chaos ransomware. Nearly 21% of the Onyx No. 1 binary relates to generic malware and known

malicious libraries. Interestingly, Onyx No. 1 contains 2.22% of the BlackBasta ransomware code. Black Basta ransomware first appeared in April 2022 (Trend Micro Research, 2022). The appearance of the BlackBasta code in the Onyx No. 1 binary may suggest that the Chaos binary was incorrectly identified as an earlier Chaos generation. Onyx ransomware was the most prominent Chaos build in April 2022.

The Onyx No. 1 does contain 2.96% identified as unique code and another 10.22% malicious library code. Onyx ransomware appears to be deeply rooted in the Chaos family, and Intezer's results suggest Onyx was modified with BlackBasta ransomware code.

Ransomware Sample	Related Families	Code Genes	Percentage
Onyx No. 1	Chaos Ransomware	43	79.64
Onyx No. 1	Generic Malware	42	9.33
Onyx No. 1	BlackBasta Ransomware	10	2.22
Onyx No. 1	Malicious Library	3	10.22

Figure 21. Onyx Genetic Summary

3.3.3. VSOP Ransomware

VSOP ransomware became the successor to Onyx. The first indication came in August 2022 when the Onyx extortion site changed the title page from Onyx to VSOP. VSOP actors post additional victims in addition to the existing Onyx victims (Cybleinc, 2022). Much like Onyx ransomware, few binary samples are seen in the wild. The VSOP victims have not released many indicators of their cyber incidents. Figure 22 represents the only VSOP sample analyzed by Intezer.

No.	Ransomware	SHA1 Hash	Source
1	VSOP	38bd5295360d1c364ed87426a97f49ebe40c9955	VirusTotal

Figure 22. VSOP Binary Metadata

Intezer indicates the VSOP binary was comprised of two ransomware samples code. Nearly 27% of the binary code was Chaos ransomware, and 7.13% was SolidBit ransomware code. However, the majority of the VSOP sample shared genes with generic malware.

VSOP shares code with UPX packer and contains unique code. Overall, VSOP was very similar to Onyx. The VSOP binary is related more to the Chaos No. 2 binary sample.

Ransomware Sample	Related Families	Code Genes	Percentage
VSOP No. 1	Generic Malware	59	80.61
VSOP No. 1	Chaos Ransomware	19	27.25
VSOP No. 1	SolidBit Ransomware	5	7.13
VSOP No. 1	Malicious Library	3	6.82

Figure 23. VSOP Genetic Summary

3.3.4. Yashma Ransomware

Yashma ransomware is the latest iteration of the Chaos family. Yashma first appeared in May 2022 and is a modified version of the Chaos 5+ builder. For example, Yashma incorporates the .Net obfuscator to better cloak itself (BlackBerry Research & Intelligence Team, 2022).

Much like the Yashma predecessors, only a few samples have been seen in the wild. Figure 24 represents two Yashma binary files sourced from VirusTotal.

No.	Ransomware	SHA1 Hash	Source
1	Yashma	878ad3025f8ea6b61ad4521782035963b3675a52	VirusTotal
2	Yashma	344f3b92716e83e24d363111b847e9ba8ffa65bc	VirusTotal

Figure 24. Yashma Binary Metadata

While both Yashma binary files had different SHA1 hashes, the Intezer genetic results were identical. Yashma No. 1 and Yashma No. 2 shared 84.85% of code specific to Yashma ransomware. Intezer indicated that Yashma No. 2 is a compressed version of Yashma No. 1. The Intezer sandbox decompressed Yashma No.2 and analyzed the statically extracted file. The analysis resulted in both binaries having the same genetic summary. VirusTotal had different detection outcomes between the files due to compression. Intezer's metadata classified binary files as the Yashma ransomware builder v1.2 (2.0.0.1).

The Yashma ransomware builder did not contain any code related to previous Chaos family ransomware. The builder had 10.08% of unique code and did not use any identifiable administrative code.

Justin Harris, justin.r.harris@hotmail.com

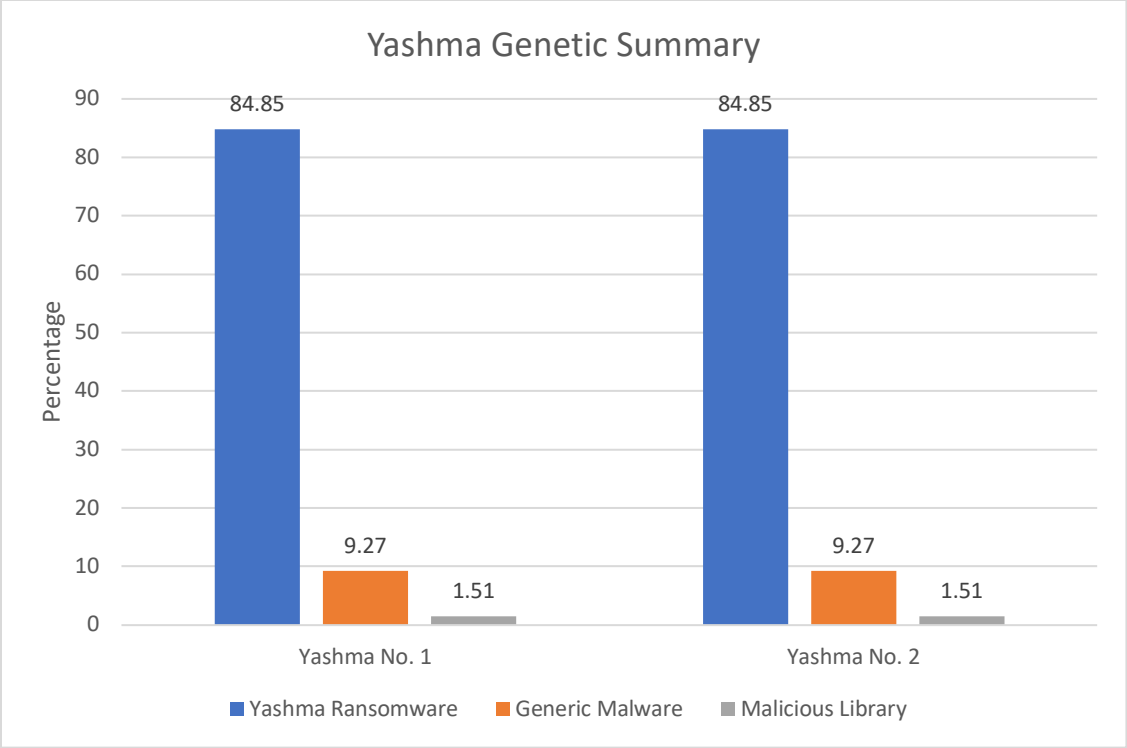

Figure 25. Yashma Genetic Summary

4. Recommendations

Genetic code analysis provides a detailed understanding of code relationships with previously known binary files. Automating the genetic analysis and ingesting the results enhances an organization's security posture. Furthermore, an organization can customize the genetic analysis to expand threat intelligence. A deeper analysis of the genetic code blocks would help link potential RaaS developers and malware authors. These links allow investigators and researchers to map a one-to-many relationship between ransomware families.

4.1. Recommendations for Implementing Genetic Analysis

Detection and threat intelligence is crucial regardless of an organizations existing incident response (IR) framework. Automating binary genetic analysis is recommended for a more robust solution to help reduce reaction time. Integrating an existing Security Information and Event Management (SIEM) or Endpoint Detection and Response (EDR) through Intezer's application programming interface (API) would provide an automated

solution. Intezer's API provides a scalable mechanism to ingest binary files with a near-real-time capability.

The genetic code comparison allows IR teams and security operation centers (SOCs) to identify code reuse between malware binaries. Understanding the relationship between these malware families will reduce false positives. Research indicated that malware binaries often share slight amounts of code outside of the primary malware family, which can cause antivirus programs to identify malicious files falsely.

Intezer's genetic code segments can be broken down into the creation of custom signatures. For example, the unique code segments could be indexed into a private library and ingested into a SIEM or EDR solution. The automated ingestion of indexed code segments would provide shareable signatures with global SOC teams.

4.2. Recommendations for Future Genetic Analysis

Ransomware and malware genetic analysis can expand beyond uses for reactive detection. A more granular exploration into a ransomware family or families could reveal common RaaS developers or link ransomware affiliates. As ransomware affiliates modify binary files, they add or replace functionality. The modified functionality begins to create a fingerprint for specific affiliates or developers. Comparing larger sample sizes would divulge more accurate links through Intezer's code genes. Organizing the binary's compile time into chronological order and mapping the genetic code changes may provide an accurate depiction of the ransomware's evolution.

Expanding research into Intezer's strings and capabilities section would yield more significant results. Cross-comparing strings and capabilities against other binary samples could solidify suspicions through empirical evidence. A unique string or capability could become a RaaS developer signature. The analysis may develop a binary fingerprint in addition to a developer fingerprint.

5. Conclusion

Ransomware as a Service (RaaS) transformed the ransomware threat landscape and proposed new challenges in ransomware attribution. Next-generation ransomware

often does not resemble early generations within multigenerational ransomware families. Intezer's binary analysis revealed several code genes that denote relationships between other known malware families. The analysis of three ransomware families confirmed that later generations often contain marginal code similarities. Some ransomware binaries did not contain any code relating to early generations. The absence of relational code can prevent outdated virus signatures from correctly identifying newly created ransomware binaries. An in-depth investigation into a binary file exhibits an interconnection between ransomware which can lead to a more accurate classification. Genetic code analysis allows organizations to look past obsolete virus signatures and correctly identify ransomware binaries. Using tools like Intezer allows investigators to adjust to the rapidly changing threat landscape and better prepare for tomorrow's threat.

Justin Harris, justin.r.harris@hotmail.com

References

Abrams, L. (2016, November 14). *Researcher finds the karma ransomware being distributed via pay-per-Install network*. BleepingComputer. https://www.bleepingcomputer.com/news/security/researcher-finds-the-karma-ransomware-being-distributed-via-pay-per-install-network/

Abrams, L. (2021, December 9). *ALPHV BlackCat - This year's most sophisticated ransomware*. BleepingComputer. https://www.bleepingcomputer.com/news/security/alphv-blackcat-this-years-most-sophisticated-ransomware/

Agcaoili, J., & Gelera, B. (2021, February 23). *An analysis of the Nefilim ransomware*. Trend Micro. https://www.trendmicro.com/en_us/research/21/b/nefilim-ransomware.html

Baker, K. (2022, February 7). *Ransomware as a service (RaaS) explained*. crowdstrike.com. https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

Bitdefender Enterprise. (2022, February 22). *What are ransomware families? (And why knowing them can help your business avoid attack)*. Business Insights Cybersecurity Blog by Bitdefender. https://businessinsights.bitdefender.com/what-are-ransomware-families-and-why-knowing-them-can-help-your-business-avoid-attack

BlackBerry Research & Intelligence Team. (2022, May 24). Yashma ransomware, tracing the chaos family tree. *BlackBerry.com*. https://blogs.blackberry.com/en/2022/05/yashma-ransomware-tracing-the-chaos-family-tree

Boczan, T., & Williams, J. (2020, March 25). SANS Webcast recap: Practical malware family identification for incident responders. *VMRay*. https://www.vmray.com/cyber-security-blog/practical-malware-family-identification-sans-webcast-recap/

Constantin, L. (2022, May 22). *Chaos ransomware explained: A rapidly evolving threat*. CSO Online. https://www.csoonline.com/article/3661633/chaos-ransomware-explained-a-rapidly-evolving-threat.html

Justin Harris, justin.r.harris@hotmail.com

Cybersecurity & Infrastructure Security Agency. (2016). *Simda Botnet*. https://www.cisa.gov/uscert/ncas/alerts/TA15-105A

Cybersecurity and Infrastructure Agency. (2021, October 18). *BlackMatter ransomware Alert (AA21-291A)*. CISA. https://www.cisa.gov/uscert/ncas/alerts/aa21-291a

Cybleinc. (2022, August 10). Onyx ransomware renames its leak site to "VSOP". *Cyble*. https://blog.cyble.com/2022/08/10/onyx-ransomware-renames-its-leak-site-to-vsop/

Dewhurst, R. (2022). *Static code analysis*. OWASP Foundation, the Open Source Foundation for Application Security | OWASP Foundation. https://owasp.org/www-community/controls/Static_Code_Analysis

Dudley, R., & Golden, D. (2022). *The ransomware hunting team: A band of misfits' improbable crusade to save the world from cybercrime*. Farrar, Straus & Giroux.

Dunn, J. (2022, May 5). Onyx ransomware damages files so even the criminals can't retrieve data. *Ransomware.org*. https://ransomware.org/blog/onyx-ransomware-damages-files-so-even-the-criminals-cant-retrieve-data/

Fortinet. (n.d.). *JuicyPotato Hacking Tool Discovered on Compromised Web Servers*. Global Leader of Cyber Security Solutions and Services | Fortinet. https://www.fortinet.com/content/dam/fortinet/assets/analyst-reports/report-juicypotato-hacking-tool-discovered.pdf

Fridman, O. (2018, December 4). Making malware human: A SANS product review. *Intezer*. https://www.intezer.com/blog/malware-analysis/sans-product-review/

Fuentes, M., Hacquebord, F., Hilt, S., Kenefick, I., Kropotov, V., McArdle, R., Mercês, F., & Sancho, D. (n.d.). *Modern Ransomware's Double Extortion Tactics and How to Protect Enterprises Against Them*. Trend Micro Research. https://documents.trendmicro.com/assets/white_papers/wp-modern-ransomwares-double-extortion-tactics.pdf

Hall, G. E. (2019, October 10). *OnyxLocker ransomware (Virus removal instructions) - Quick decryption solution*. Security and spyware news. https://www.2-spyware.com/remove-onyxlocker-ransomware.html

Hill, J. (2022, August 22). Anatomy of a SolidBit ransomware attack. *Varonis: We Protect Data*. https://www.varonis.com/blog/anatomy-of-a-solidbit-ransomware-attack

Intezer. (n.d.). *Genetic Summary Section*. https://support.intezer.com/hc/en-us/articles/360021348600-Genetic-Summary-Section

Marks, J., & Schaffer, A. (2022, May 6). *One year ago, Colonial Pipeline changed the cyber landscape forever*. The Washington Post. https://www.washingtonpost.com/politics/2022/05/06/one-year-ago-colonial-pipeline-changed-cyber-landscape-forever/

Microsoft Defender Threat Intelligence. (2022, June 13). The many lives of BlackCat ransomware. *Microsoft Security Blog*. https://www.microsoft.com/en-us/security/blog/2022/06/13/the-many-lives-of-blackcat-ransomware/

Nuce, J., Kennelly, J., Goody, K., Moore, A., Rahman, A., Williams, M., McKeague, B., & Wilson, J. (2021, November 4). Shining a light on DARKSIDE ransomware operations. *Mandiant*. https://www.mandiant.com/resources/blog/shining-a-light-on-darkside-ransomware-operations

Qasem, A., Shirani, P., Debbabi, M., Wang, L., Lebel, B., & Agba, B. L. (2022). Automatic vulnerability detection in embedded devices and firmware. *ACM Computing Surveys*, *54*(2), 1-42. https://doi.org/10.1145/3432893

Rosenberg, J. (2021, March 22). Examining code reuse reveals undiscovered links among North Korea's malware families. *Intezer*. https://www.intezer.com/blog/research/examining-code-reuse-reveals-undiscovered-links-among-north-koreas-malware-families/

Sinitsyn, F. (2021, May 25). *Evolution of JSWorm ransomware*. Securelist | Kaspersky's threat research and reports. https://securelist.com/evolution-of-jsworm-ransomware/102428/

Smith, B. (2021, September 14). *Chaos ransomware: Reviewing the newbie — How to fix guide*. How To Fix Guide. https://howtofix.guide/chaos-ransomware/

Sophos. (2022). *The State of Ransomware 2022*. https://www.sophos.com/en-us/content/state-of-ransomware

Justin Harris, justin.r.harris@hotmail.com

Symantec. (2022, September 22). Noberus ransomware: Darkside and BlackMatter successor continues to evolve its tactics. *Symantec Enterprise Blogs*. https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/noberus-blackcat-ransomware-ttps

Tancio, B. (2022). *Adversary Emulation: Nefilim Ransomware vs. Security Onion* [Master's thesis]. https://www.sans.org/white-papers/

Terefos, A. (2021, October 18). *Karma ransomware | An emerging threat with a hint of Nemty pedigree*. SentinelOne. https://www.sentinelone.com/labs/karma-ransomware-an-emerging-threat-with-a-hint-of-nemty-pedigree/

Toulas, B. (2021, October 19). *New karma ransomware group likely a Nemty rebrand*. BleepingComputer. https://www.bleepingcomputer.com/news/security/new-karma-ransomware-group-likely-a-nemty-rebrand/

Trend Micro Research. (2022, September 1). Ransomware spotlight: Black basta. *#1 in Cloud Security & Endpoint Cybersecurity | Trend Micro*. https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-blackbasta

Trend Micro. (2018, September 27). *DanaBot Banking Trojan Found Targeting European Countries*. https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/danabot-banking-trojan-found-targeting-european-countries

Trend Micro. (2019, August 5). *ENTSCRYPT aka GermanWiper, SYRK, and STOP Ransomware Variants Usher in August*. #1 in Cloud Security & Endpoint Cybersecurity | Trend Micro. https://www.trendmicro.com/vinfo/hk-en/security/news/cybercrime-and-digital-threats/entscrypt-aka-germanwiper-syrk-and-stop-ransomware-variants-usher-in-august

U.S. Department of State. (2021, November 4). *DarkSide ransomware as a service (RaaS)*. United States Department of State. https://www.state.gov/darkside-ransomware-as-a-service-raas/

The White House. (2021, May 11). *FACT SHEET: The Biden-Harris administration has launched an all-of-Government effort to address colonial pipeline incident*. https://www.whitehouse.gov/briefing-room/statements-releases/2021/05/11/fact-

sheet-the-biden-harris-administration-has-launched-an-all-of-government-effort-to-address-colonial-pipeline-incident