

■ JANUARY 2022

ARMOR



THREAT INTELLIGENCE REPORT

THE EVOLUTION OF DOPPEL SPIDER FROM BITPAYMER TO GRIEF RANSOMWARE

A detailed link analysis of BitPaymer, DoppelPaymer, and Grief ransomware throughout the years.

AMER ELSAD

Threat Intelligence Analyst | Threat Resistance Unit

CONTENTS

INTRODUCTION

The ransomware industry has continued to evolve during the past couple of years. And it is still a growing problem in 2021, as ransom demands become larger, attackers smarter, and intrusions longer. Ransomware threat actors are hitting U.S. and global companies harder with more effective ransomware deployments resulting in a more devastating impact to victim organizations. Most ransomware operators are now conducting full-scale network intrusions such as the one recently done by an Advanced Persistent Threat (APT). When they strike, they deploy ransomware across the entirety of victim organizations, often with devastating consequences, and their deployments are more complete and more effective.

One ransomware variant that we have been tracking is called Grief ransomware, which is the latest version of DoppelPaymer ransomware and previously known as BitPaymer ransomware. This ransomware has gained a lot of popularity recently due to its continuous improvement and its large number of victims in the U.S. and global companies.

Another reason we focused on this particular ransomware is that it shares the same code with several other identified ransomware such as WastedLocker and Macaw, and with Dridex (downloader malware). This indicates that Grief was very likely created by the same team that created Dridex, which, according to the U.S. Treasury, is Evil Corp, also known as Indrik Spider and TA505. The Treasury also mentioned in a recent report that Evil Corp is led by Maksim Yakubets who has worked for the Russian Federal Security Service (FSB), including on projects intended to “acquire confidential documents through cyber-enabled means.”¹ Yakubets is also on the FBI’s Most Wanted list.

So Grief, being a product of Evil Corp, probably launched and transitioned to the Grief brand so Evil Corp could evade authorities and prevent organizations from realizing they are breaking OFAC sanctions by paying them². It should be noted that this isn’t the first time Evil Corp had rebranded its malware in an apparent attempt to evade sanctions.

In this report we will dive deep and explore Grief operation and development since it was first observed in July 2017 as BitPaymer, as well as compare the different variants and partnerships with other threat actors and ransomware groups.



AMER ELSAD
Threat Intelligence Analyst

Amer Elsad serves as a Threat Intelligence Analyst II in the Threat Resistance Unit for Armor, where he focuses on Adversary Tracking, including their behaviors, objectives, campaigns, and tactics, techniques, and procedures (TTPs). Elsad is also responsible for evaluating customer telemetry and analyzing intrusion activity by advanced attackers. Prior to joining Armor, he worked in both private and government domains, and has broad experience in threat intelligence, threat hunting, and malware analysis. Elsad holds a bachelor’s degree in Information Systems from Alexandria University.

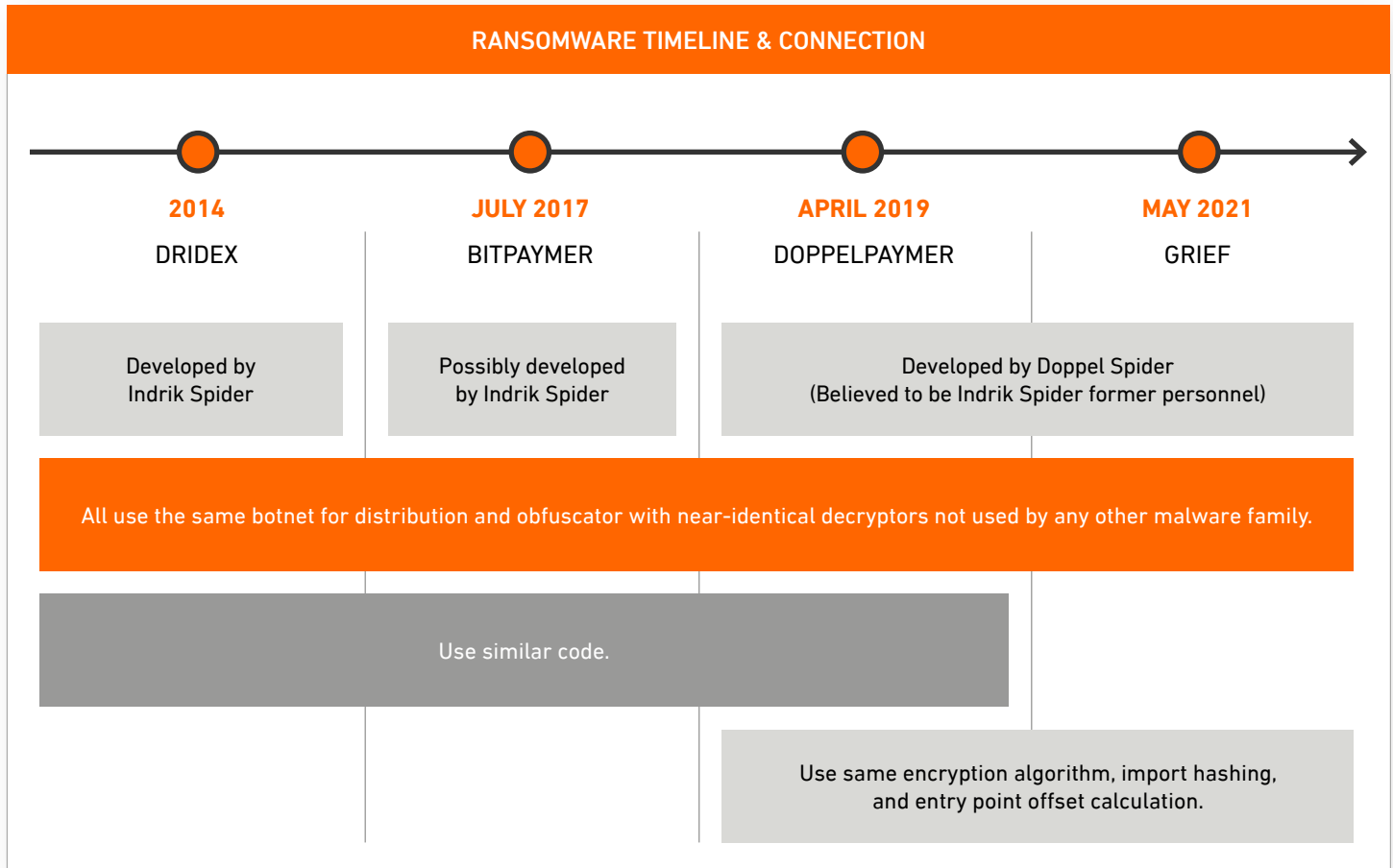
WHAT IS GRIEF, PREVIOUSLY KNOWN AS DOPPELPAYMER?

Grief is a ransomware-as-a-service (RaaS) operation, which refers to a business model where operators develop crypto-locking malware. Affiliates then use the malware to infect victims—with both operators and affiliates sharing the profits.

Grief emerged in May 2021 and was considered a new operation at first. But later it was discovered that the Grief gang carries many similarities to the DoppelPaymer variant. This led to the conclusion that Grief ransomware is, in fact, the latest version of DoppelPaymer ransomware with just minor code changes and a new cosmetic theme. The threat group behind it also has been very active since the release of Grief.

Grief and DoppelPaymer ransomware were both developed by Doppel Spider, a threat actor affiliated with Evil Corp and first discovered by CrowdStrike. This variant has several technical overlaps with Doppel Spider’s multi-toolset that provides a definitive link to the adversary, such as DoppelPaymer, BitPaymer, and Dridex.

According to its report on Doppel Spider, CrowdStrike has assessed with high confidence that a new group likely has split off from Indrik Spider a.k.a. Evil Corp³. Furthermore, Grief’s operator has a dedicated data leak site reachable only via the anonymizing Tor browser.



SIMILARITIES BETWEEN GRIEF & DOPPELPAYMER & EVIDENCE SUPPORTING THEY ARE THE SAME OPERATION

In early May 2021, DoppelPaymer ransomware activity dropped significantly, and there has not been a new victim post since May 6, 2021. In addition, no victim posts have been updated since the end of June, and no files have been leaked since June 25. However, the operation appears to have been rebranded under the name Grief (a.k.a. Pay OR Grief) by its operator, Evil Corp, in an attempt to avoid sanctions imposed on the crime group in December 2019 by the U.S. Treasury Department's Office of Foreign Assets Control.¹

Despite the threat actor's effort to make Grief look like a separate RaaS, the similarities to DoppelPaymer are so striking, in our opinion, that a connection between the two is impossible to dismiss. There is so little setting the two apart, and it's mostly cosmetic. We strongly believe that it's the same operation under a different name.

SIMILARITIES

- When Grief was first spotted in the wild, DoppelPaymer and Grief showed to encrypt files in the same manner: "identical encryption algorithms (2048-bit RSA and 256-bit AES), import hashing, and entry point offset calculation." Both also have used the Dridex botnet for distribution.
- Grief's ransomware executable was first compiled on May 17 and included Grief's crypto-locking code and note, but it directed victims to DoppelPaymer's payment portal.
- Both Grief and DoppelPaymer use the European Union's General Data Protection Regulation (GDPR) as a warning that non-paying victims would still have to face legal penalties due to the breach.

DIFFERENCES

- One change from DoppelPaymer is that the group previously demanded payment in bitcoin, and now Grief wants victims to pay in monero (a more privacy-preserving cryptocurrency). That may be because the FBI was able to successfully recover some of the bitcoin Colonial Pipeline paid to DarkSide.
- Unlike DoppelPaymer, Grief malware samples have the ProcessHacker binaries removed. But it uses the same code to decrypt data from binary's data section.
- Grief's string encryption algorithm is the same as DoppelPaymer, i.e., 2048-bit RSA and 256-bit AES, except the RC4 key length that was increased to 48 bytes from 40 bytes.



THE DIFFERENCES SEEM TO BE MOSTLY COSMETIC

Both ransomware leak sites are nearly identical, including shared code that displays a captcha to prevent automated crawling as shown in Figure 1 and Figure 2.

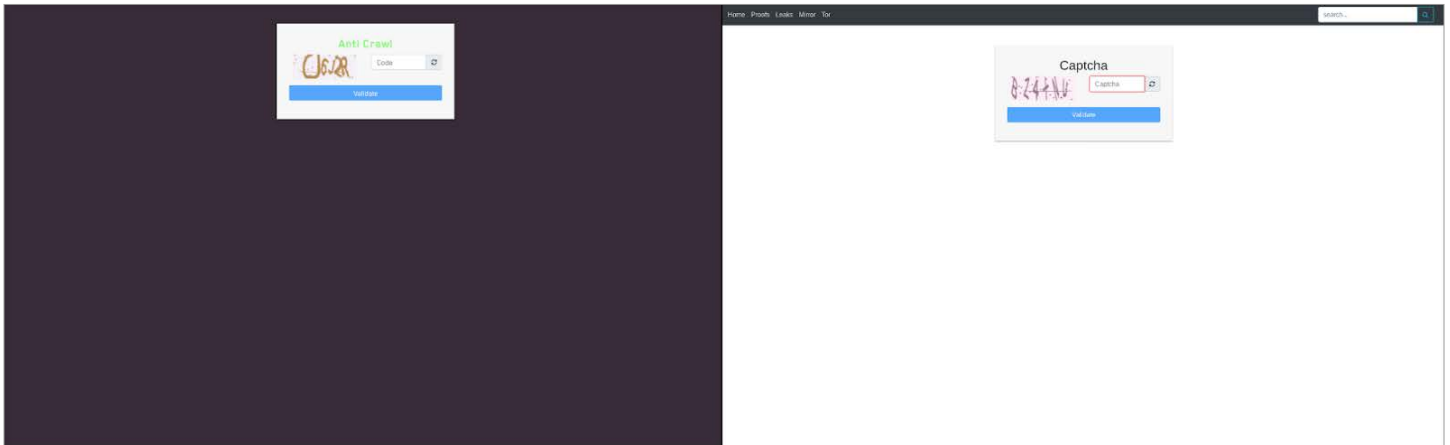


Figure 1. Grief ransomware (left) and DoppelPaymer (right) captcha (Source: zscaler)

The victim-specific leak page layouts are also identical as shown below in Figure 2 containing the victim's URL, organizational description, images of stolen data, example stolen data files, and a list of machines that were compromised.

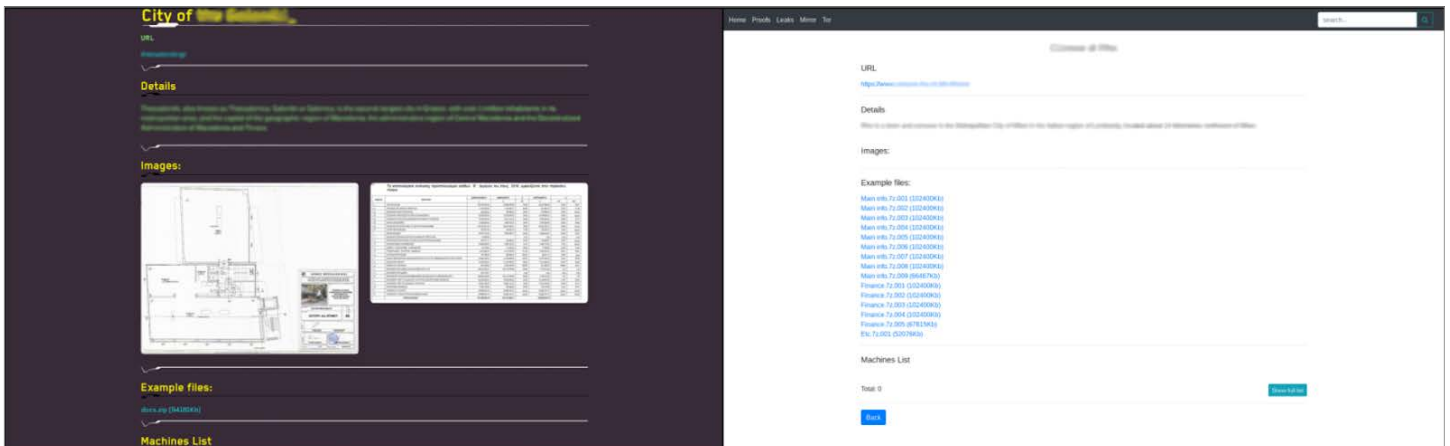


Figure 2. Grief ransomware (left) and DoppelPaymer (right) victim leak pages (Source: zscaler)

SIMILARITIES BETWEEN BITPAYMER & DOPPELPAYMER

DoppelPaymer was considered to be based on the BitPaymer ransomware (which first emerged in 2017) due to the connections in their code, ransom notes, and payment portals. In July 2019, CrowdStrike highlighted some similarities between BitPaymer and DoppelPaymer, speculating that DoppelPaymer appears to be the work of the former BitPaymer group members but is a bit more complex.³

BitPaymer, also known as FriedEx or IEncrypt, was initially dubbed BitPaymer based on text in its ransom demand web site. This ransomware was discovered in early July 2017 by Michael Gillespie and in use since at least July 2017.⁴ It is manually operated and used against private and public entities in targeted attacks. Research from ESET showed BitPaymer and Dridex are sharing multiple technical similarities.

SIMILARITIES

- BitPaymer ransomware contains the same referenced string between Dridex and DoppelPaymer aimed to act as an anti-Windows Defender emulator checking the existence of the file, "C:\aaa_TouchMeNot_.txt," which is indicative of Windows Defender sandbox activity.
- DoppelPaymer ransomware contains a peculiar string reused across samples from BitPaymer and Dridex as shown below in Figure 3. It copies the unicode string "setup runn" to eax via lstrcpyW API call. discovered by SentinelOne.⁵

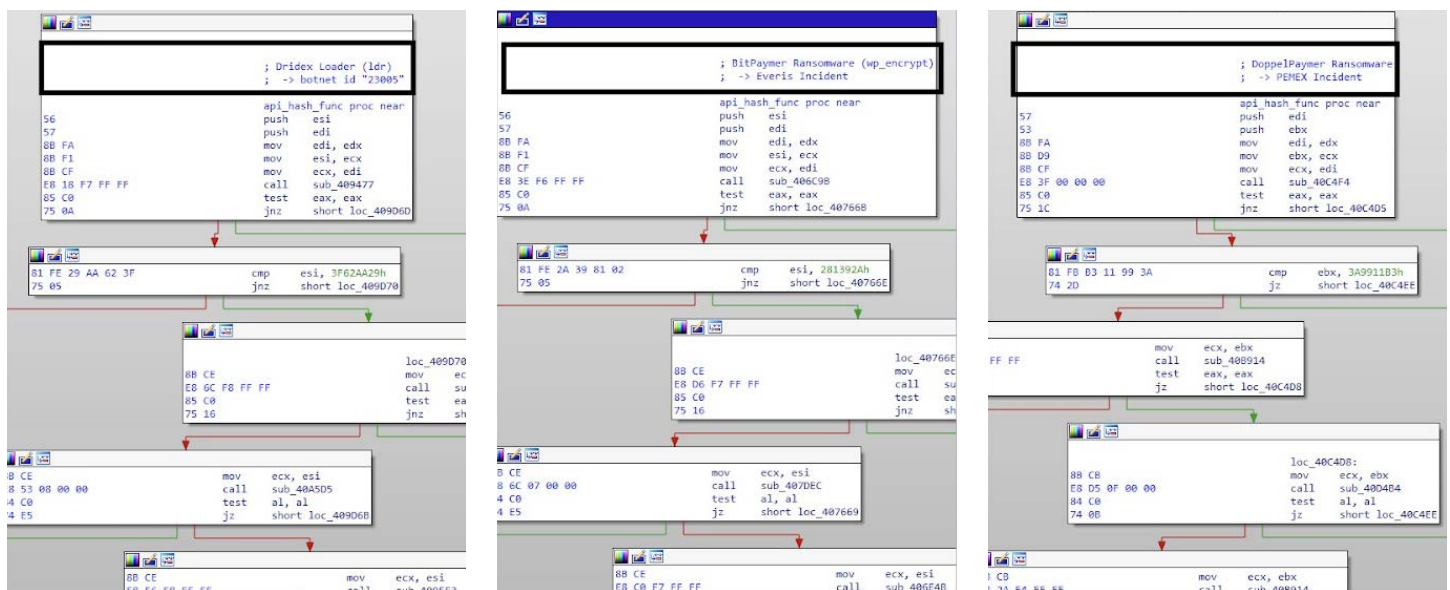


Figure 3. Code reuse between Dridex (left), BitPaymer (center), and DoppelPaymer (right). (Source: Sentinelone).

DIFFERENCES

- DoppelPaymer uses 2048-bit RSA + 256-bit AES for encryption, while BitPaymer uses 4096-bit RSA + 256-bit AES (with older versions using 1024-bit RSA + 128-bit RC4). Furthermore, DoppelPaymer improves upon BitPaymer's rate of encryption by using threaded file encryption.
- ESET discovered a second variant dubbed FriedEx, which focuses on higher profile targets and companies rather than regular end users, and is usually delivered via an RDP brute force attack.⁶ The ransomware encrypts each file with a randomly generated RC4 key, which is then encrypted using a hardcoded 1024-bit RSA public key and saved in the corresponding. readme_txt file.

DOPPELPAYMER & BITPAYMER SIMILARITIES WITH DRIDEX

The Dridex banking trojan first appeared in 2014 as a relatively simple bot inspired by older projects, but quickly turned into one of the most sophisticated banking trojans on the market. The development seems to be steady, with new versions of the bot, including minor fixes and updates, being released on a weekly basis with occasional breaks. From time to time, the authors introduce a major update that adds some crucial functionality or larger changes.

SIMILARITIES

- It should be noted that all the ransomware variants we mentioned above are deployed via Dridex. They all use the same custom obfuscator as Dridex—which is an obfuscator not used by any other malware families—and they all have near-identical decryptors.
- As we mentioned above, DoppelPaymer was derived from BitPaymer. It was discovered later by CrowdStrike that some Evil Corp personnel that developed Dridex separated into a threat group called Doppel Spider and attempted an attack using DoppelPaymer. It is also known that the same group developed DoppelDridex, known as Dridex 2.0 version. The overall information can be seen in CERT-FR's CTI report.⁷
- A Dridex loader sample was distributed through the Emotet malware on June 4, 2019. The Dridex sample contained code to decrypt either a 32-bit or a 64-bit core bot module from its sdata section using the exact same encryption, compression, and data format that DoppelPaymer uses to extract PEs from its sdata section. This observation ties this Dridex variant directly with DoppelPaymer.
- BitPaymer uses the same techniques as Dridex to hide as much information as possible about its behavior.
- It resolves all system API calls on the fly by searching for them by hash, stores all strings in encrypted form, looks up registry keys and values by hash, etc.
- Analysis results of CrowdStrike show that Dridex malware and BitPaymer ransomware were found in identical incidents, which strengthens the fact that it must be the same developing group.⁸

As per Figure 4, part of a function used for generating UserID was found across all Dridex binaries (both loaders and bot modules). The very same Dridex-specific function is also used in the BitPaymer binaries. The function produces the same results—it generates a string from several attributes of the victim’s machine that serves as a unique identifier of the given victim.

This kind of similarity to Dridex is present throughout the BitPaymer a.k.a. FriedEx binaries, and only very few functions that correspond to the specific ransomware functionality are not found in the Dridex sample (i.e., the file encryption loop and creation of ransom message files).

As we can see in Figure 5, another shared feature is the order of the functions in the binaries, which occurs when the same codebase or static library is used in multiple projects. While the BitPaymer sample seems to be missing some of the functions present in the Dridex sample and vice versa—which is caused by the compiler omitting unreferenced/unused functions—the order remains the same.

```

v14 = Buffer::GetSize(v41);
Buffer::Resize(v41, v14 + 4);
v15 = Buffer::GetSize(v41);
v16 = Buffer::GetWritePtrAt(v41, v15 - 4);
v17 = *(&v37 + v13++);
*v16 = v17;
}
while ( v13 < 4 );
Reg::GetPathByHash(&v43, v41, HKEY_LOCAL_MACHINE, 0);
if ( v42 )
    sub_CA10B0(v42, 1);
Buffer::Cleanup(v41);
v18 = Reg::GetValueByHash(&v43, &v29, 0xCD48FA82);
v19 = Reg::QueryDWORD(&v43, *v18);
String::Cleanup(&v29);
v28 = v19;
if ( a4 )
{
    v29 = v19;
    Buffer::Write(v36, &v29, 4);
    v29 = v6;
    Buffer::Write(v36, &v29, 2);
}
else
{
    v29 = v6;
    Buffer::Write(v36, &v29, 2);
    v29 = v28;
    Buffer::Write(v36, &v29, 4);
}
v29 = a3;
Buffer::Write(v36, &v29, 2);
v20 = Buffer::GetSize(v36);
v21 = Buffer::GetWritePtrAt(v36, 0);
Util::HashData(&v37, v21, v20);
v22 = Util::BinToHex(&v37, v21, v20);
String::ToLowerCase(v22, &v34);
String::Cleanup(&v29);
Buffer::Cleanup(&v37);
if ( v6 )
{
    String::FromArray(v5, &v34);
}
else
{
    WString::Init(&v32, 128);
    v28 = v33 >> 1;
    v23 = GetAPIByHash(kernel132, GetComputerNameW);
    if ( v23 )
        v23(v32, &v28);
    Util::WStringToAscii_0(v35, v32);
    v24 = v34;
    v25 = String::AppendChar(v35, '_');
    String::Join(v25, v24);
    String::FromArray(v5, v35);
    String::Cleanup(v35);
    String::Cleanup(&v32);
}
}
v14 = Buffer::GetSize(v41);
Buffer::Resize(v41, v14 + 4);
v15 = Buffer::GetSize(v41);
v16 = Buffer::GetWritePtrAt(v41, v15 - 4);
v17 = *(&v37 + v13++);
*v16 = v17;
}
while ( v13 < 4 );
Reg::GetPathByHash(&v43, v41, HKEY_LOCAL_MACHINE, 0);
if ( v42 )
    sub_2A1093(v42, 1);
Buffer::Cleanup(v41);
v18 = Reg::GetValueByHash(&v43, &v29, 0xCD48FA82);
v19 = Reg::QueryDWORD(&v43, *v18);
String::Cleanup(&v29);
v28 = v19;
if ( a4 )
{
    v29 = v19;
    Buffer::Write(v36, &v29, 4);
    v29 = v6;
    Buffer::Write(v36, &v29, 2);
}
else
{
    v29 = v6;
    Buffer::Write(v36, &v29, 2);
    v29 = v28;
    Buffer::Write(v36, &v29, 4);
}
v29 = a3;
Buffer::Write(v36, &v29, 2);
v20 = Buffer::GetSize(v36);
v21 = Buffer::GetWritePtrAt(v36, 0);
Util::HashData(&v37, v21, v20);
v22 = Util::BinToHex(&v37, v21, v20);
String::ToLowerCase(v22, &v34);
String::Cleanup(&v29);
Buffer::Cleanup(&v37);
if ( v6 )
{
    String::FromArray(v5, &v34);
}
else
{
    WString::Init(&v32, 128);
    v28 = v33 >> 1;
    v23 = GetAPIByHash(kernel132, GetComputerNameW);
    if ( v23 )
        v23(v32, &v28);
    Util::WStringToAscii_0(v35, v32);
    v24 = v34;
    v25 = String::AppendChar(v35, '_');
    String::Join(v25, v24);
    String::FromArray(v5, v35);
    String::Cleanup(v35);
    String::Cleanup(&v32);
}
}
    
```

Figure 4. Comparison of GetUserID function present in both Dridex (left) and BitPaymer (right) samples. (Source: ESET)

Note: (sub_CA5191 and sub_2A56A2, etc.) are auto-generated function name pairs. Based on code addresses, they do not match, but the code they refer to does.

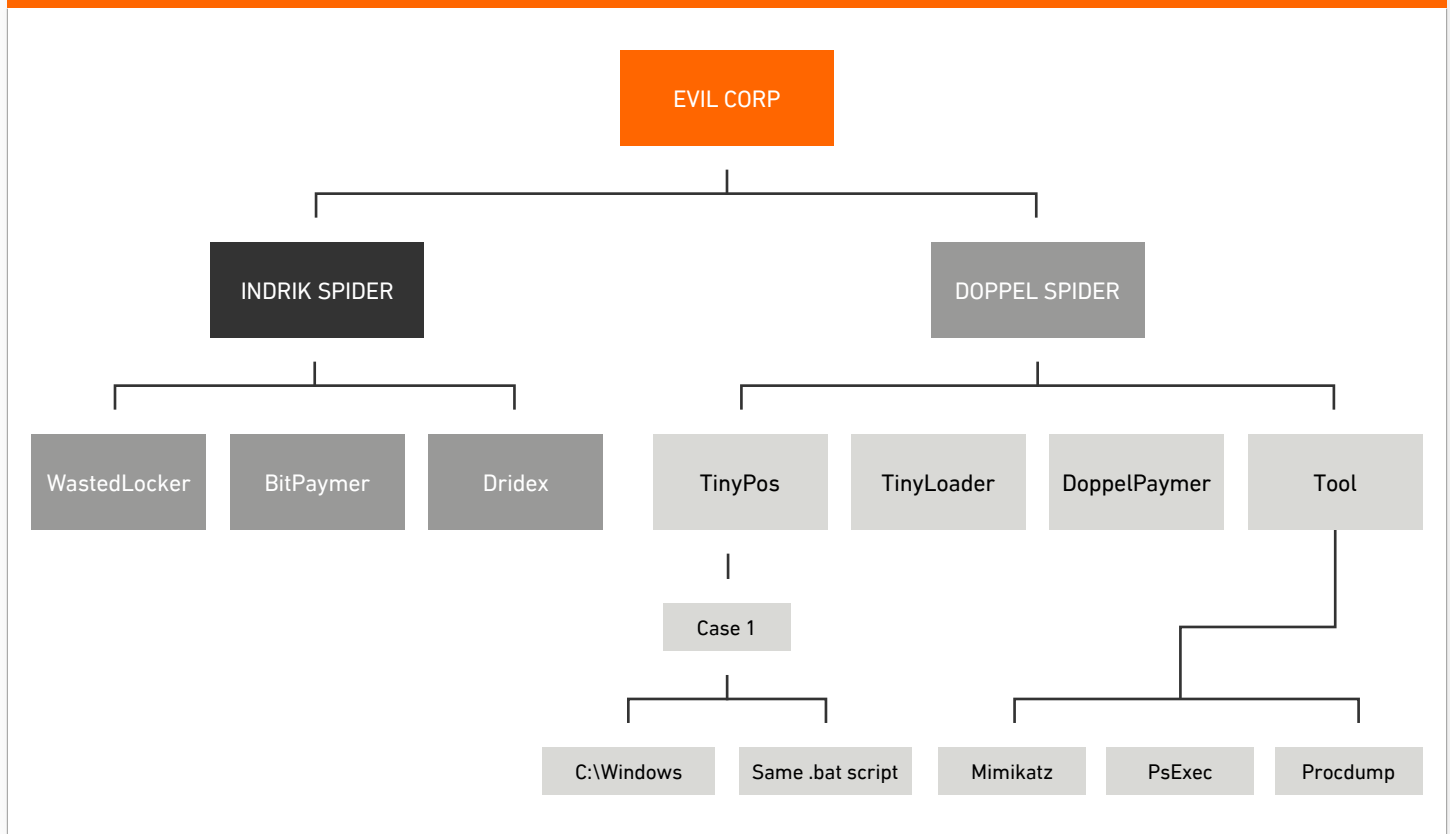
Function name	Segment	Function name	Segment
Core_GetUserIDInternal	.text	Core_GetUserIDInternal	.text
sub_CA5191	.text	sub_2A56A2	.text
sub_CA51A7	.text	sub_2A58F0	.text
sub_CA53F5	.text	Buffer_Init	.text
Buffer_Init	.text	sub_2A5952	.text
sub_CA5457	.text	Buffer_Cleanup	.text
Buffer_Cleanup	.text	Buffer_Copy	.text
Buffer_Copy	.text	Buffer_GetWritePtrAt	.text
sub_CA54C8	.text	Buffer_Write	.text
sub_CA5508	.text	Util_BinToHex	.text
Buffer_GetWritePtrAt	.text	sub_2A5ABF	.text
Buffer_Write	.text	sub_2A5AD4	.text
Util_BinToHex	.text	Buffer_Write_0	.text
sub_CA5616	.text	sub_2A5C0C	.text
sub_CA562B	.text	Crypto_GenRandomData	.text
sub_CA563A	.text	Buffer_InitInternal	.text
sub_CA5642	.text	sub_2A5DA0	.text
Buffer_Write_0	.text	Buffer_Resize	.text
sub_CA56C0	.text	Buffer_GetSize	.text
sub_CA56DA	.text	MemsetWrapper_0	.text
sub_CA5757	.text	String_FromCharArray	.text
Crypto_GenRandomData	.text	String_Init	.text
Buffer_InitInternal	.text	sub_2A5E1D	.text
sub_CA581B	.text	sub_2A5E3A	.text
Buffer_Resize	.text	WString_Init	.text
Buffer_GetSize	.text		
String_FromCharArray	.text		
String_Init	.text		
sub_CA5898	.text		
sub_CA58B5	.text		
WString_Init	.text		

Figure 5. Comparison of function order in Dridex (left) and BitPaymer (right) samples. Functions that are missing in the other sample are highlighted in the corresponding color. (Source: ESET)

CONNECTIONS WITH OTHER RANSOMWARE GROUPS — WHO IS THE OPERATOR OF THE RANSOMWARE?

Blockchain analysis by Insights shows a connection between five of 2020's biggest ransomware strains: Maze, Egregor, SunCrypt, wastedLocker, and DoppelPaymer.⁹ Insights has pointed out that many RaaS affiliates carrying out attacks switch between different strains, and research also reveals that seemingly distinct strains are likely controlled by the same people.

CONNECTION BETWEEN FOUR OF 2020'S BIGGEST RANSOMWARE STRAINS



Currently, Evil Corp is mainly used to refer to Indrik Spider, and it attempts to attack using WastedLocker instead of the BitPaymer. It is also believed that Doppel Spider is a group that has split off from Indrik Spider. However, we can assume close relation between the two organizations by the above-mentioned facts.

SPLIT WITHIN EVIL CORP

In April 2019, Evil Corp is thought to have split into two groups: Indrik Spider and Doppel Spider. While Indrik Spider allegedly ran the malware Dridex and BitPaymer, as had been done since 2018, Doppel Spider purportedly executed a modified version of Dridex, DoppelDridex, and a variant of the ransomware BitPaymer—DoppelPaymer. In this way, it not only deployed banking fraud campaigns via DoppelDridex, but also ransomware campaigns via DoppelPaymer.

GIVEN THAT:

- The malware FakeUpdates distributed Dridex in October 2019, and that Dridex deployed either BitPaymer or DoppelPaymer within the victims' Integrated Security Systems (ISS).
- During a DoppelPaymer incident, FireEye detected the downloading of Dridex v4 botnet ID 501 (associated with Evil Corp), and then of Dridex v2 botnet ID 12333 in a bid to deploy DoppelPaymer (associated with Doppel Spider).
- Doppel Spider uses the services of Emotet, as does Evil Corp. It would appear that the two groups are continuing to collaborate, or perhaps even that Doppel Spider is a subgroup of Evil Corp.
- However, since the first quarter of 2020, what distinguishes the operators behind DoppelPaymer from BitPaymer's operators is that those of the former have started to publish the data exfiltrated from the IS of their victims (on the website [www.doppleshare\[.\]top/](http://www.doppleshare[.]top/)) in the same way as operators of other ransomware (Maze, Sodinokibi, Clop, and Nemty, in particular).



HISTORY OF PARTNERSHIP WITH OTHER THREAT ACTORS & MALWARE FAMILIES

PARTNERSHIP WITH QAKBOT

During 2020, Mandiant observed multiple DoppelPaymer ransomware deployments where initial access was achieved through widespread use of QakBot malware.¹⁰ In contrast to REvil's affiliate model where individual threat actors are responsible for end-to-end intrusions from initial access to ransomware deployment, QakBot and DoppelPaymer employ a partnership model where one threat actor is responsible for initial access, privilege escalation, and lateral movement, and then it is passed to another threat actor for ransomware deployment of Dridex, DoppelDridex, and a variant of the ransomware BitPaymer—DoppelPaymer. In this way, it not only deployed banking fraud campaigns via DoppelDridex, but also ransomware campaigns via DoppelPaymer.

PARTNERSHIP WITH LOCKEAN THREAT ACTOR

A comprehensive report published by France's Computer Emergency Response Team (CERT-FR), a division of ANSSI, the country's national cybersecurity agency, investigated a threat actor dubbed Lockean, and it is believed they may also be a DoppelPaymer affiliate for the following reasons:¹¹

- Strains of the DoppelPaymer ransomware were also distributed from the same IP address that Lockean has used in their campaigns, such as Maze ransomware, according to a code analysis platform done by Cert-FR.
- In DoppelPaymer incidents observed by Cer-FR at Fareva, the ransomware strain was named "k166sm.exe," which matches the naming convention used for the DoppelPaymer strains hosted on the IP address « 185.238.0.233 ». As such, it is possible that it was involved in the incident at Fareva.
- Akamai typosquatting Cobalt Strike C2s (« atakai-technologies.host », « akamai-technologies.site » and « akamai-technologies.space ») were found in incidents leading to encryption by DoppelPaymer, thereby supplementing the ANSSI's observations about the DoppelPaymer incidents at Company A and Fareva.
- DoppelPaymer was already distributed by QakBot. The renaming of QakBot as « md.exe », specific to the « domain » affiliate and therefore to Lockean, was found during the DoppelPaymer incident at Company A in June 2020.

PARTNERSHIP WITH TINYLOADER

According to Talos' report released in November 2019, DoppelPaymer, TinyPoS, SVCHOST SAMPLE, etc., were distributed from the same server used for TinyLoader.¹² SVCHOST SAMPLE also was identical to TinyLoader. That is, TinyLoader, TinyPoS, and DoppelPaymer were distributed together from one server.



TACTICS, TECHNIQUES, & PROCEDURES (TTPs)

Many ransomware families are being distributed through RaaS programs, and since each has multiple affiliates, there may be shifts in TTPs used by threat actors. Some ransomware (e.g., REvil, Netwalker, and DarkSide) were public. DoppelPaymer and Grief were not, and their TTPs shifts were minimal.

We looked into all previous variants and campaigns of the ransomware and its operator Doppel Spider to try to identify patterns as well as the use of TTPs and common tools to help us better defend and predict what the attacker will be using in their attacks. We noticed that they have shifted and used a combination of TTPs and other post exploitation tools similar with other ransomware, including some living off the land techniques such as alternate data streams (ADS), which we discussed in our previous [blog](#).

Based on our research, we have put together a combination of the TTPs we have observed the attacker using for their campaigns.

Since Dridex is likely to download Grief/DoppelPaymer ransomware as a second payload, it is also worth focusing detection efforts on that. We suggest reading these great resource and analysis of Dridex: "The Malware Dridex: Origins and Uses"⁷ and "New Dridex Variant Being Spread By Crafted Excel Document."¹³



DISTRIBUTION & INITIAL ACCESS

- We've observed the ransomware being distributed through multiple methods, which confirms our theory that Grief/DoppelPaymer is sold on black markets as a RaaS (ransomware-as-a-service) and used by different threat actors, designated as "affiliates."
- But all of them tend to favor malicious email attachments as the initial vector for infiltrating a victim's network. This is typically done using highly targeted spear-phishing emails that make victims more likely to open attachments under the guise that the emails come from a trusted source. The attachment includes either JavaScript or VBScript, which is responsible for downloading other malware with more advanced capabilities (such as Emotet) into the victim's system.



EXECUTION

- Once Emotet is downloaded, it will communicate with command-and-control (C&C) to download and execute Dridex malware, which in turn is used to download either Grief directly or tools such as PowerShell Empire, Cobalt Strike, PsExec, and Mimikatz, to steal credentials, move laterally, or execute different commands, such as disabling security software.
- Once Dridex enters the system, these threat actors do not immediately deploy the ransomware. Instead, they will try to move laterally within the affected system's network to find a high-value target to steal critical information from. That's because the success of attacks relies on whether campaign operators manage to gain control over domain accounts with elevated privileges after establishing initial access.



RECONNAISSANCE

- After obtaining adequate credentials, attackers perform extensive reconnaissance of machines and running software to identify targets for ransomware delivery. They use the built-in command `qwinsta` to check for active RDP sessions, run tools that query Active Directory or LDAP, and ping multiple machines. In some cases, the attackers target machines that are running systems management software.



LATERAL MOVEMENT AND ELEVATING PRIVILEGES

- It has been reported that threat actors propagated manually for approximately one week within the victim's network before the ransomware deployment. To perform the propagation, they first sought to compromise network administrators accounts to take control of central servers, such as Active Directory. These accounts serve also to identify critical resources within the network (file system storage, data backup, production-related equipment, etc.).
- Use of group policies, binaries placed in SYSVOL locations and deployed across the domain using scripts, has been reported:
 - PsExec
 - BITS Jobs
 - Scheduled Tasks
- Attackers utilize various methods to gain access to privileged accounts, including common credential theft tools such as Mimikatz and LaZagne. They have also been observed using Sysinternals tool ProcDump to obtain credentials from LSASS process memory. They have even used LSASecretsView to access credentials stored in the LSA secrets portion of the registry, which is accessible to local admins (this portion of the registry can reveal credentials for domain accounts used to run scheduled tasks and services).



- They have used a technique introduced by @enigma0x3 (See Figure 6), which is Fileless UAC bypass¹⁴. It changes the registry key - 'HKCR\mscfile\shell\open\command' default value to point at the '.cmd' file, which will cause Grief to run with high privileges without a UAC prompt. If it fails in elevating its privileges, it will exit without encrypting the file system. The abuse of eventvwr.exe and similar types of registry hijack elevation techniques are a serious architecture weakness and are very popular among malware. It is also easy to tweak the technique to bypass any existing detection solution.
- When running with high privileges, Grief deletes shadow copy files from the host. It does this by running the command 'vssadmin.exe Delete Shadows /All /Quiet' and 'diskshadow.exe /s %TEMP%\<tempfile>.tmp' (<tempfile>.tmp = "delete shadows all\r\nexit\r\n") for Windows Server versions.
- Next, it tries to take ownership of a random service by using 'takeown.exe /F <service_name>' and 'icacls.exe <service_name> /reset'. It then replaces the service with a copy of its own and executes Grief as a service. After successfully hijacking and running from a service, it begins to encrypt the file system.
- It has been reported that Grief, in some cases, will not destroy shadow copies (T1490 Inhibit System Recovery). Its reason could be that the operator will want to delete shadow copies manually.

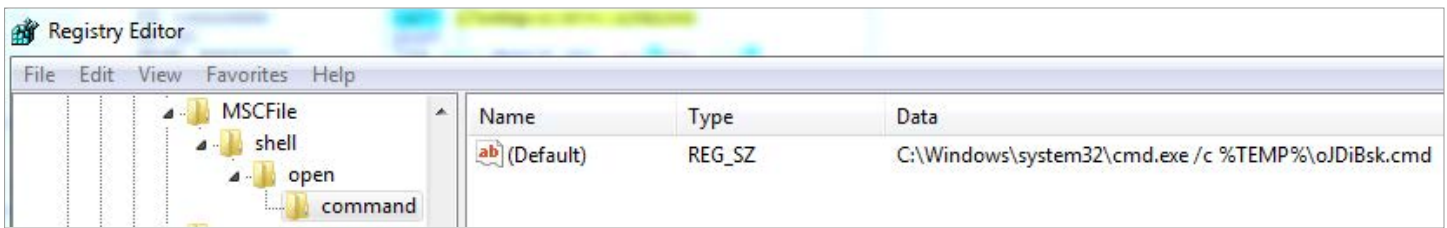


Figure 6: Compromised registry key (Source: Morphisec)



PERSISTENCE

- The threat actor has been observed adjusting a legitimate Windows Service configuration to run the malware. Grief chooses a legitimate Windows Service and replaces the ImagePath registry value of the service's configuration to execute the ransomware again at the next boot (T1543.003 Create or Modify System Process: Windows Service)¹⁵. It guarantees that the next time the system begins, Grief operates again and returns the system to safe mode.
 - File: <random>.exe
 - Path: %APPDATA%\<random>.exe
 - Note: Copy of Grief binary
 - Service: <random_service>
 - Path: %WINDIR%\system32\<random_service>.exe
 - Note: Ransomware Service
 - Service: <random_service>-1
 - Path: %WINDIR%\system32\<random_service>.exe-1
 - Note: Backup of Service



DEFENSE EVASION

- The threat actors have used NTFS file attributes T1564.004 to hide their malicious payloads.¹⁶
- They used an anti-Windows Defender emulator checking the existence of the file "C:aaa_TouchMeNot_.txt," which is indicative of Windows Defender sandbox activity that checks if it is running as an alternate data stream (See Figure 7). It does that by checking if the name of the file on the disk ends with:

```
configuration->running_as_a_service = running_as_a_service;
AllocBuffer(&filePath, *&v78.Length);
GetModuleFileNameW = GetProcAddressCustom(0x461BAD0A, 0x23FBBC5);
if ( GetModuleFileNameW )
    GetModuleFileNameW(0, filePath, v89 >> 1);
baseName = getBaseNameInUnicode_BT_wrapper(&filePath, &a1[1], '\\');
ADS = wcschr_wrapper(baseName, ':'); // Check if file name has ':' in it
```

Figure 7: Check if running from alternate data stream (Source: Morphisec)

- If not, it will copy itself to a hidden alternate data stream under "%APPDATA%\<random_name>:BIN" and create a new process with the old file path as a parameter.
- The alternate data stream process then performs the following:
 - Deletes the original file
 - Copies itself from :BIN alternate data stream to a hidden directory in %APPDATA%\<random>.exe.
 - Creates a temporary '.cmd' file in %temp% directory and writes the following (Figure 8).

```
oJDiBsk.cmd
1 start /b %APPDATA%\Roaming\EATEHQ~1\SedN8B2.exe %APPDATA%\Roaming\W4WH2Y~1
2 del %0 & exit
```

Figure 8: Cmd file that will be executed from registry (Source: Morphisec)

- Some of its variants used in many attacks are signed using what appears to be stolen certificates from OFFERS CLOUD LTD, which may be trusted by various security solutions.



IMPACT

- They deploy the ransomware over the weekend and night—first on DC servers as critical resources, including on data backup systems, to maximize impact.
- They change user passwords before forcing a system restart into safe mode to prevent user entry from the system. They then change the notice text that appears before Windows proceeds to the login screen.
- They used <http://MediaFire.com> for exfiltration via a web browser.
- Other TTPs include: gaining access to Hyper Visors and spinning up new virtual machines to launch the ransomware from inside them. They spun up a few different VMs logged into them, disabled defender, and then launched the ransomware from the desktop. They then used that to encrypt the vhd files on the host. (This means that the VM is using a bridged interface to do this in order to spread across network while evading PSPs.)
- For Grief to set the system to boot from safe mode with minimum services available and no network connectivity is remarkable because very few ransomware families do this.
- They used ProcessHacker to terminate different services on endpoint devices that may interfere with file encryption. They also used an interesting technique for this method where the application is bundled with a kernel driver that can be used to terminate processes and services.



VICTIMOLOGY

DoppelPaymer was used in over 125 ransomware incidents in 2020.

DoppelPaymer Gang was one of the most active ransomware groups, claiming to have infected 186 companies and public entities between 2019 and May 1, 2021. DoppelPaymer is considered one of the top ransomware groups, coming in just behind the Sodin/REvil, Conti/Ryuk, Black Matter (formerly Darkside), and CLOP groups.

MOST NOTABLE INCIDENTS OF ALL THE RANSOMWARE VARIANTS



Aug. 25, 2017

BitPaymer notably compromised multiple Scottish hospitals as well as targeted entities in education, manufacturing, finance, and agriculture.









Aug. 1, 2018

Matanuska-Susitna, a borough of Anchorage, Alaska, was infected with the Emotet trojan and subsequently infected with the BitPaymer ransomware, forcing the borough to use typewriters for a week.¹⁷

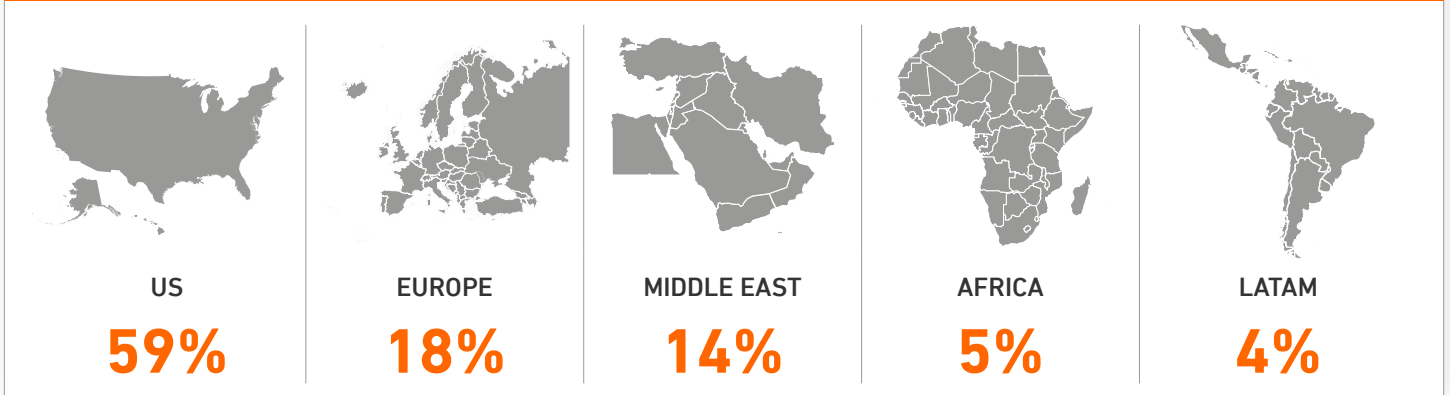


Aug. 8, 2018

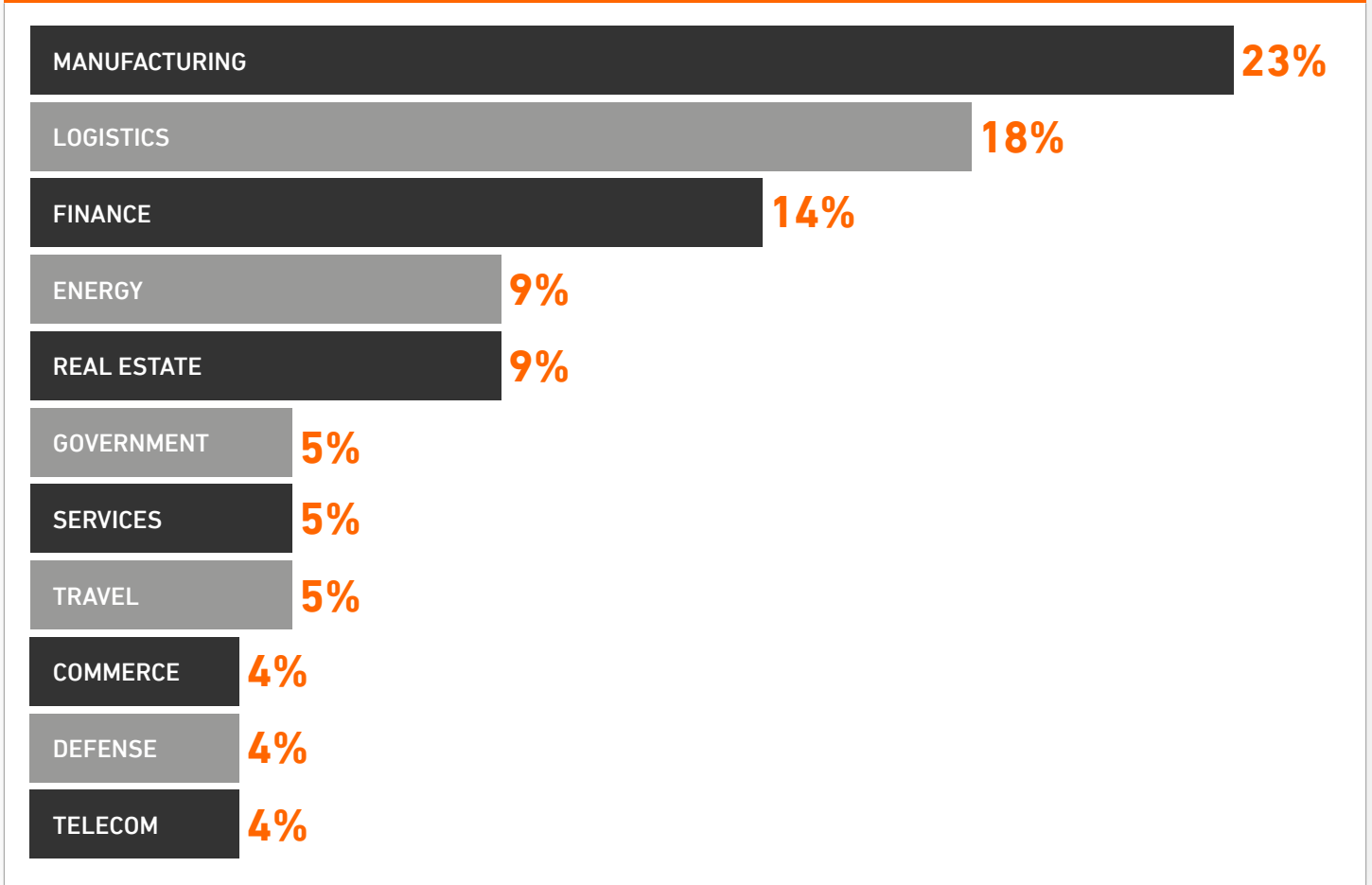
PGA of America was likely infected with a BitPaymer variant.¹⁸

	<p>July 18, 2019</p> <p>An ongoing BitPaymer campaign targeted at least 15 U.S. small and medium-sized businesses (SMBs) spanning across the financial, agricultural, technology, and government sectors over the last three months. The infection began with an email containing Dridex, which was used to collect network information. BitPaymer appeared to be deployed during a weekend while employees were away and proliferated once employees returned.¹⁹</p>
	<p>Oct. 10, 2019</p> <p>The actors behind BitPaymer exploited a zero-day vulnerability in iTunes for Windows to evade detection on compromised systems.²⁰</p>
	<p>Nov. 12, 2019</p> <p>Pemex, Mexico's state-owned oil company, recently suffered a DoppelPaymer ransomware attack that demanded \$4.9 million USD in order to decrypt their files.²¹</p>
	<p>Sept. 18, 2020</p> <p>The most known and discussed victim of DoppelPaymer ransomware was one against Düsseldorf University Clinic in Germany in September 2020. The actors actually wanted to target the Düsseldorf University and addressed it in the ransom note, but ended up hitting the hospital. When the perpetrators were made aware, they sent a digital key to get the hospital up and running again. But that ransomware infection led to the death of one patient who the hospital was unable to treat on arrival. She died in an ambulance while being transported to another medical facility with functioning systems. The threat actors also fixed their sights on a county E911 center as well as another community college in the same month.²²</p>
	<p>Dec. 15, 2020</p> <p>The FBI issued a warning regarding DoppelPaymer, a ransomware family that first appeared in 2019 when it launched attacks against organizations in critical industries. Its activities continued throughout 2020, including a spate of incidents in the second half of the year that left its victims struggling to properly carry out their business operations. According to the FBI notification, DoppelPaymer's primary targets were organizations in healthcare, emergency services, and education. The ransomware already had been involved in a number of attacks in 2020, including disruptions to a community college as well as police and emergency services in a city in the U.S. during the middle of the year.²³</p>
	<p>May 27, 2021</p> <p>The Grief Ransomware Gang (a rebrand of the DoppelPaymer Ransomware Group) claimed to have infected 41 new victims between May 27, 2021, and Oct. 1, 2021, with their ransomware. Over half the companies listed on Grief's underground leak site were based in the U.K. and Europe. The Grief Ransomware Gang appeared to have altered its motus operandi (MO), targeting more corporate and public entities in the U.K. and Europe than the United States. They also seemed to be backing away from U.S. hospitals and emergency healthcare services, previously a top target for them.²⁴</p>

GEOGRAPHIC DISTRIBUTION OF TARGETS



INDUSTRY DISTRIBUTION OF TARGETS



SOURCES

1. [“Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware” – December 5, 2019](#)
2. [“Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments” – September 21, 2021](#)
3. [“BitPaymer Source Code Fork: Meet DoppelPaymer Ransomware and Dridex 2.0” – July 12, 2019](#)
4. [“Just got sample of “Bit paymer” #ransomware. Ext “.locked” w/ marker, drops “.readme.txt” for every encrypted file. https://virustotal.com/file/d693c33dd550529f3634e3c7e53d82df70c9d4fbd0c339dbc1849ada9e539ea2/analysis/1499719839/.” Gillespie, Michael \[@demonslay335\], Twitter, July 10, 2017](#)
5. [“YARA Hunting for Code Reuse: DoppelPaymer Ransomware & Dridex Families” – November 14, 2019](#)
6. [“FriedEx: BitPaymer ransomware the work of Dridex authors” – May 2, 2018](#)
7. [“The Malware Dridex: Origins and Uses” – July 17, 2020](#)
8. [“Big Game Hunting: The Evolution of INDRIK SPIDER From Dridex Wire Fraud to BitPaymer Targeted Ransomware” – November 14, 2018](#)
9. [“Blockchain Analysis Shows Connections Between Four of 2020’s Biggest Ransomware Strains” – February 4, 2021](#)
10. [“The Evolving Maturity in Ransomware Operations” – December 2020](#)
11. [“Identification of a new cybercriminal group : Lockean” – November 3, 2021](#)
12. [“C2 With It All: From Ransomware To Carding” – November 4, 2019](#)
13. [“New Dridex Variant Being Spread By Crafted Excel Document” – September 10, 2021](#)
14. [“Fileless, UAC Bypass Using Eventvwr.exe and Registry Hijacking” – August 15, 2016](#)
15. [“Create or Modify System Process: Windows Service” – January 17, 2020](#)
16. [“Hide Artifacts: NTFS File Attributes” – March 13, 2020](#)
17. [“The MSB 2018 Virus Situation” – July 30, 2018](#)
18. [“Hackers target PGA servers, seek Bitcoin ransom” – August 8, 2018](#)
19. [“BitPaymer targets 15 U.S. organizations in 3 months, researchers say” – July 18, 2019](#)
20. [“Apple Zero-Day Exploited in new BitPaymer Campaign” – October 10, 2019](#)
21. [“Mexico’s Pemex Oil Suffers Ransomware Attack, \\$4.9 Million Demanded” – November 12, 2019](#)
22. [“Woman dies after hospital is unable to treat her during crippling ransomware infection, cops launch probe” – September 18, 2020](#)
23. [“Private Industry Notification” – December 10, 2020](#)
24. [“Ransomware gang threatens to wipe decryption key if negotiator hired” – September 15, 2021](#)



[ARMOR.COM](https://armor.com) | (US) +1 844 682 2858 | (UK) +44 800 500 3167

22010107 Copyright © 2022. Armor, Inc., All rights reserved.