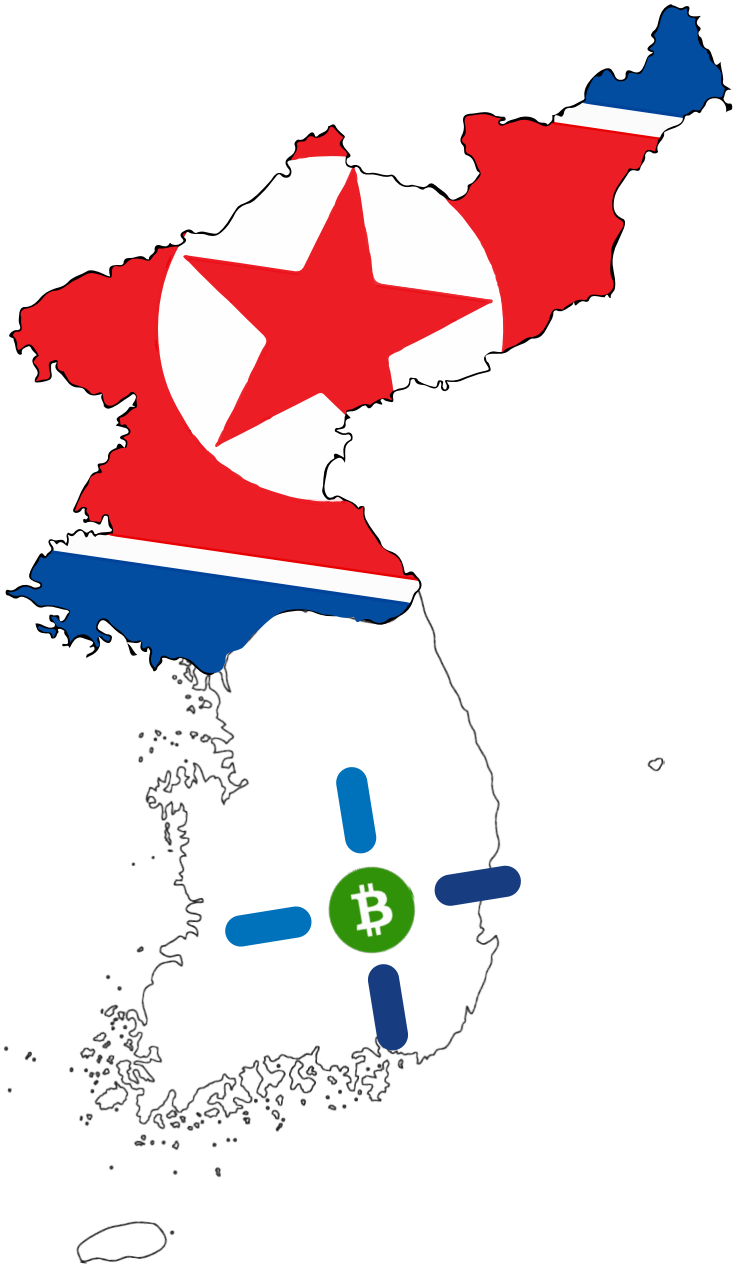
Recorded Future

REPORT

North Korea Targeted South Korean Cryptocurrency Users and Exchange in Late 2017 Campaign

By Juan Andres Guerrero-Saade and Priscilla Moriuchi
Recorded Future



CTA-2018-0116

Recorded Future

North Korea Targeted South Korean Cryptocurrency Users and Exchange in Late 2017 Campaign

Executive Summary

North Korea continued to target South Korea through late 2017 with a spear phishing campaign against both cryptocurrency users and exchanges, as well as South Korean college students interested in foreign affairs. The malware in this campaign utilizes a known Ghostscript exploit (CVE-2017-8291— Intel Card) and is tailored to target only users of a Korean language word processor, Hancom's Hangul Word Processor.

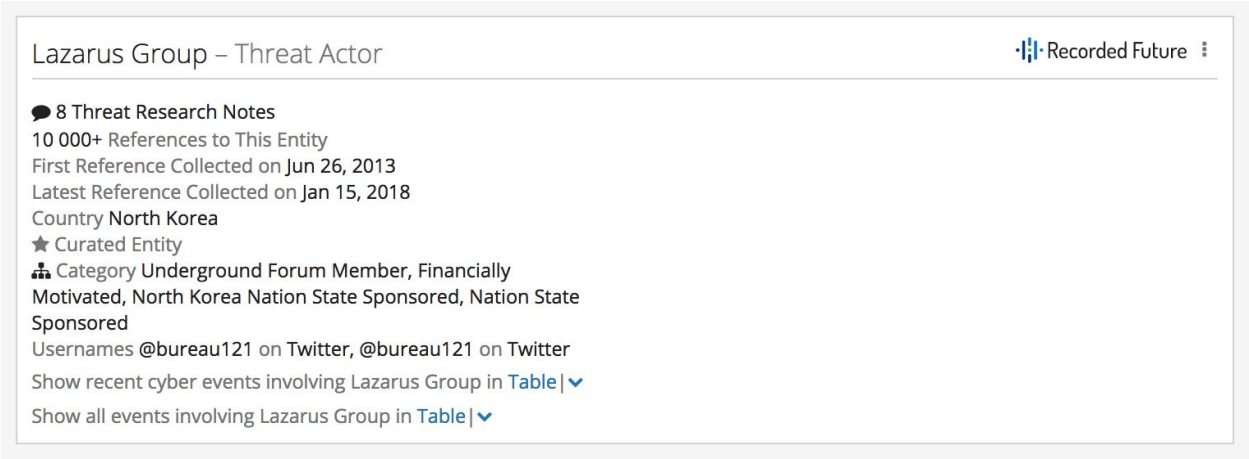
Key Judgments

- North Korean government actors, specifically Lazarus Group (Intel Card), continued to target South Korean cryptocurrency exchanges and users in late 2017, before Kim Jong Un's New Year's speech and subsequent North-South dialogue.
- This campaign also targeted South Korean college students interested in foreign affairs and part of a group called "Friends of MOFA" (Ministry of Foreign Affairs).
- The malware employed shared code with Destover malware (Intel Card), which was used against Sony Pictures Entertainment in 2014 and the first WannaCry victim in February 2017.
- The dropper in this campaign exploited a known Ghostscript vulnerability, CVE-2017-8291. The exploit implementation includes Chinese terms possibly signifying an attempted false flag or a Chinese exploit supplier.

Background

North Korean state-sponsored cyber operations are largely clustered within the Lazarus Group (Intel Card) umbrella. Also known as HIDDEN COBRA by the U.S. government, Lazarus Group has conducted operations since at least 2009, when they launched a DDoS attack on U.S. and South Korean websites utilizing the MYDOOM worm. Until 2015, Lazarus Group cyber activities primarily focused on South Korean and U.S. governments and financial organizations, including destructive attacks on South Korean banking and media sectors in 2013 and the highly publicized attack on Sony Pictures Entertainment in 2014.

Beginning in 2016, researchers discovered a shift in North Korean operations toward attacks against financial institutions designed to steal money and generate funds for the Kim regime.



Lazarus Group in Recorded Future. Access the complete Intel Card here.

By 2017, North Korean actors had jumped on the cryptocurrency bandwagon. The first known North Korean cryptocurrency operation occurred in February 2017, with the theft of $7 million (at the time) in cryptocurrency from South Korean exchange Bithumb. By the end of 2017, several researchers had reported additional spear phishing campaigns against South Korean cryptocurrency exchanges, numerous successful thefts, and even Bitcoin and Monero mining. North Korea also utilized Bitcoin for the global WannaCry ransomware attack in mid-May, forcing victims to pay ransom in Bitcoin.

Threat Analysis

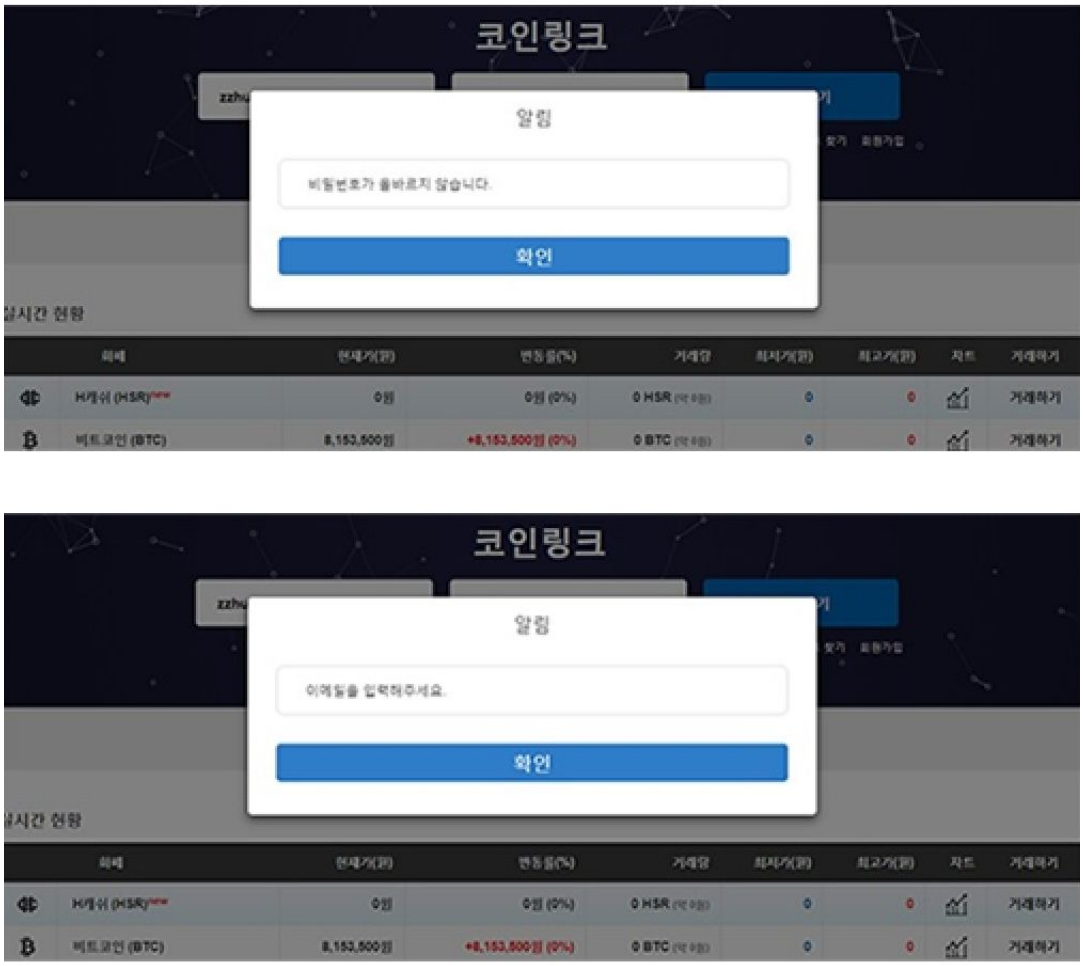
Insikt Group researchers regularly follow North Korean threat actors through a variety of methods, one of which includes proactive monitoring of attack vectors based on software disproportionately adopted in South Korea. Using this methodology, we identified a recent Lazarus Group malware campaign, which likely began late Fall 2017. Lazarus Group

operations target a wide swath of countries and verticals, with a particular interest in South Korean targets.

Recent reporting regarding North Korean attacks against cryptocurrency exchanges and using Pyeongchang Olympics as a lure describe techniques that are unusual for the Lazarus Group. These include leveraging PowerShell, HTA, JavaScript, and Python, none of which are common in Lazarus operations over the last eight years. The campaign we discovered showcases a clear use of Lazarus TTPs to target cryptocurrency exchanges and social institutions in South Korea.

This campaign leveraged four different lures and targeted Korean-speaking users of the Hangul Word Processor (.hwp file extension), a Korean-language word processing program utilized widely in South Korea. North Korean state-sponsored actors have used Hangul exploits (CVE-2015-6585) and malicious .hwp files in the past, including during a phishing campaign in early 2017, to target South Korean users.

Beyond Korean-speaking HWP users, targets of this campaign appear to be users of the Coinlink cryptocurrency exchange, South Korean cryptocurrency exchanges at large (or at least those that are hiring), and a group called "Friends of MOFA" (Ministry of Foreign Affairs), which is a group of college students from around South Korea with "a keen interest in foreign affairs."



Payload shows two prompts from coinlink.co.kr, the first tells the user their password is incorrect, the second asks for their email address.

The first cryptocurrency-focused lure appears designed to obtain the emails and passwords of users of Coinlink, a cryptocurrency exchange run by the South Korean electronic stock exchange KOSDAQ.

The second and third appear to be resumes stolen from two actual South Korean computer scientists, both with work experience at South Korean cryptocurrency exchanges.

The fourth document was lifted from a blog run by the South Korean group "Friends of MOFA" detailing a Korean Day celebration in late September 2017 during which President Moon Jae-in spoke about the importance of the Korean diaspora and the upcoming Winter Olympics in Pyeongchang.

세계한인의 날 알아보기

모파랑 독자 여러분, 안녕하세요. Friends of MOFA 11기 현승희 입니다.
9월 27일 오전 서울 송파구 롯데호텔월드에서는 '제11회 세계한인의 날 기념식 및 2017 세계한인회장대회 개회식'이 문재인 대통령의 참석 하에 있었습니다.

이날 기념식에 참석한 문재인 대통령은 서용달 모모야마가루인대학 대학원 명예교수에게 국민훈장 무궁화장을 수여하였습니다.

또한 이희범 평창올림픽조직위원장과 함께 남창규 유럽한인총연합회 회장, 오공택 재일민단 중앙본부단장에게 대형 평창올림픽 배지를 전달한 후 기념촬영을 하였습니다.

여러분은 '세계 한인의 날'에 대하여 잘 아시는가요?

그럼 이제부터 '세계 한인의 날'에 대하여 알아보려 가도록 하겠습니다.

우리 정부는 2007년 처음으로 10월 5일을 '세계 한인의 날'을 제정했습니다. 700만 재외동포를 위한 기념일 제정은 동포들의 오랜 염원이 실현된 것입니다.

문민정부의 재외동포재단 설립, 국민의 정부의 재외동포법 제정에 이은 참여정부의 '세계 한인의 날'제정은 정부의 재외동포정책에 새로운 이정표를 세운 것으로 되지 않을까요?

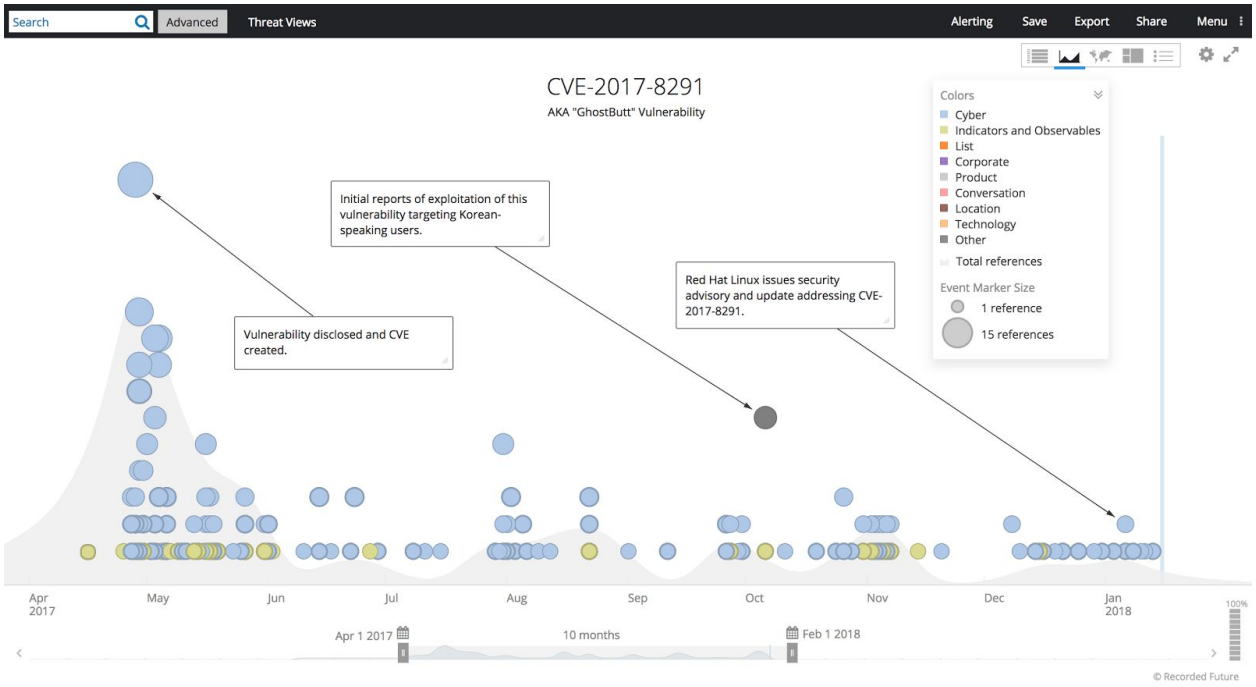
우리 민족의 이주 역사는 세계열강이 식민지 개척에 앞을 다투던 1860년대에 살길을 찾아 러시아, 중국, 일본, 하와이로 향했던 선조들에 의해 시작되었습니다.
우리 민족의 이주 역사는 불행했던 과거사의 반증이었습니다.

This document is from a blog post from the "Friends of MOFA" (Ministry of Foreign Affairs) detailing a Korean Day celebration attended by President Moon Jae-in.[1]

Technical Analysis

This campaign relies on a known Ghostscript exploit (CVE-2017-8291) that can be triggered from within an embedded PostScript in a Hangul Word Processor document.

[1] Note: All Korean language translations provided by Gerald Kim.



Timeline of CVE-2017-8291 exploitation.

```
%!PS-Adobe-3.0
/yinzi.{.token.pop.exch.pop.}.bind.def
/yaoshi.<B889008C>.def.
/yima{.
→   /funcA.exch.def.
→   .0.1.funcA.length.1.sub.{.
→   →   /funcB.exch.def.
→   →   funcA.funcB.2.copy.get.yaoshi.funcB.4.mod.get.xor.put.
→   }.for.
→   funcA.
}.def.
```

Screenshot of the function names utilized in the PostScript.

Our initial finding focused on "로그인 오류.hwp" or "Korean Day" lure, but once we created a signature for the particular implementation of the PostScript, we found three additional lure documents in a public malware repository tied together by the use of this exploit: two CVs and a cryptocurrency exchange-themed lure. All were created in the span of a month from mid-October to late November. Despite a nearly identical delivery mechanism (with the exception of altered 4-byte XOR keys), the payloads (when recoverable) were different in each case.

- It's worth noting that the function names used in the PostScript are transliterated Chinese words. While "yima" (decode) and "yaoshi" (key) appear appropriate in their functional context, the word "yinzi" (factor/money) does not. The latter may be obscure technical slang or be a misuse signifying a potential false flag.

This would not be the first time the Lazarus Group used foreign-language terms to misdirect attribution efforts; BAE researchers discovered transliterated Russian terms in previous Lazarus operations. However, an alternate explanation may point to a Chinese exploit supplier or the language competency of the developer.

The attack chain occurs in multiple stages with the PostScript deobfuscating a first stage shellcode that's been XORed with a hardcoded four-byte key. The shellcode in turn triggers the GhostScript vulnerability in order to execute an embedded DLL that has also been XORed. A PwnCode.Club blogpost details the deobfuscation of the shellcode and loading of the DLL into memory.

Lazarus malware families (like Hangman (Intel Card), Duuzer (Intel Card), Volgmer (Intel Card), SpaSpe (Intel Card), etc.) overlap, likely as the result of the developers cutting-and-splicing an extensive codebase of malicious functionality to generate payloads as needed. This erratic composition make the Lazarus intrusion malware difficult to identify and group or cluster, unless they are analyzed at the level of code similarity.

Upon deobfuscating the payloads, we found 32-bit DLLs built in part on the Destover malware (Intel Card) code. Destover has been used in a number of North Korea-attributed operations: most infamously against Sony Pictures Entertainment in 2014, the Polish banking attacks in January 2017, and the first WannaCry victim in February 2017.

This campaign relies on multiple payloads fashioned out of the Destover infostealer code to collect information about the victim system and exfiltrate files. Each payload contains an embedded 64-bit version of itself. The payloads accompanying the newer cryptocurrency exchange-themed lure docs compiled a month after the Korean Day payload further obfuscate their functionality by resolving imports at runtime.

This type of obfuscation is common in the Lazarus Hangman malware family. They also rely entirely on IPs (rather than domains) for their command-and-control infrastructure, a tactic likely borne of the use of hacked servers for infrastructure.

Outlook

This late 2017 campaign is a continuation of North Korea's interest in cryptocurrency, which we now know encompasses a broad range of activities including mining, ransomware, and

outright theft. Outside of the May WannaCry attack, the majority of North Korean cryptocurrency operations have targeted South Korean users and exchanges, but we expect this trend to change in 2018. We assess that as South Korea responds to these attempted thefts by increasing security (and possibly banning cryptocurrency trading) they will become harder targets, forcing North Korean actors to look to exchanges and users in other countries as well.

Further, while this campaign and toolset are specific to the Hangul Word Processor, the vulnerability it exploited (CVE-2017-8291) is not. This vulnerability is for the Ghostscript suite and affects a wide range of products, and while this particular version is triggered from within an embedded PostScript in an HWP document, it could easily be adapted to other software.

As South Korean exchanges harden their networks and the government imposes stricter regulatory controls on cryptocurrencies, exchanges and users in other countries should be aware of the increased threat level from North Korean actors.

Appendix A

Indicators of Compromise

Lures

MD5	SHA256
da02193fc7f2a628770382d9b39fe8e0	3cfc7666c97c38f38a3b3ec1d132f2836ade7e6e6e3cddb30b0d7d81682de0b2
3d0d71fdedfd8945d78b64cdf0fb11ed	3e9eab029c52ac34b91f906c8f92ad9059531f825905260023764f8a069edbbf
63069c9bcc4f8e16412ea1a25f3edf14	396a684949c96815b54c8e4c2fafbe6324d8c4dde2c9294411658fb5209cd70c
8152e241b3f1fdb85d21bfcf2aa8ab1d	1cc7ad407fc87acb9c961105943c87a7bd77c4d4cc90b84b46fb5dcf779b50fd

Payloads

46d1d1f6e396a1908471e8a8d8b38417	3368b6060d181e39a57759ab9b7f01221e0cd3a397000977aa8bb07a0e6a94ca
6b061267c7ddeb160368128a933d38be	ca70aa2f89bee0c22ebc18bd5569e542f09d3c4a060b094ec6abeeeb4768a143
afa40517d264d1b03ac5c4d2fef8fc32	f94fb5028a81177bb5ea3428349da4d9b125f81adb658df40d6e8f3ea0e0e3e7
c270eb96deaf27dd2598bc4e9afd99da	cf065e50a5bef24099599af6a60a78c1607a04b21d3573a25ab26bf044a119d6
d897b4b8e729a408f64911524e8647db	5afa8329c0a159811b55c92303f0d0b9b8834843c76f51777593d414bda5191b
e1cc2dcb40e729b2b61cf436d20d8ee5	77cee0ccc739d3d420e95460c72f7ad2a9846f06e4a7089fb92b8fca4a52ce3f

Command-and-Control

110.173.188.53:443
70.60.36.183:443
72.10.122.70:443
112.160.75.159:5443
125.142.192.81:443
175.213.42.234:443

Yara Rules

```
rule apt_NK_Lazarus_SKOlympics_EPS
{
	meta:
		author = "JAG-S, Insikt Group, RF"
		desc = "CN terms in PostScript loader"
		TLP = "Green"
		version = "1.0"
		md5 = "231fe349faa7342f33402c562f93a270"

	strings:
		$eps_strings1 = "/yinzi { token pop exch pop } bind def" ascii wide
		$eps_strings2 = "/yaoshi <A3E6E7BB> def" ascii wide
		$eps_strings8 = /\/yaoshi <[A-F0-9]{8}> def/ ascii wide
		$eps_strings3 = "/yima{" ascii wide
		$eps_strings4 = "/funcA exch def" ascii wide
		$eps_strings5 = "0 1 funcA length 1 sub {" ascii wide
		$eps_strings6 = "/funcB exch def" ascii wide
		$eps_strings7 = "funcA funcB 2 copy get yaoshi funcB 4 mod get xor put"
ascii wide

	condition:
		6 of them
}
```

```
rule apt_NK_Lazarus_Fall2017_payload_minCondition
{
    meta:
        desc = "Minimal condition set to detect payloads from Fall 2017 Lazarus
Campaign against Cryptocurrency Exchanges and Friends of MOFA 11"
        author = "JAGS, Insikt Group, Recorded Future"
        version = "2.0"
```

```
        TLP = "Green"
        md5 = "46d1d1f6e396a1908471e8a8d8b38417"
        md5 = "6b061267c7ddeb160368128a933d38be"
        md5 = "afa40517d264d1b03ac5c4d2fef8fc32"
        md5 = "c270eb96deaf27dd2598bc4e9afd99da"
        md5 = "d897b4b8e729a408f64911524e8647db"
        md5 = "e1cc2dcb40e729b2b61cf436d20d8ee5"

    strings:
        $sub1800115A0 =
{488D542460488D8DB005000041FF9424882000004C8BE84883F8FF0F84EA010000488D8DC007000033D
241B800400000E8}
        $sub18000A720 = {33C0488BBC2498020000488B9C2490020000488B8D600100004833CCE8}

    condition:
        uint16(0) == 0x5A4D and filesize < 5MB
        and
        any of them
}
```