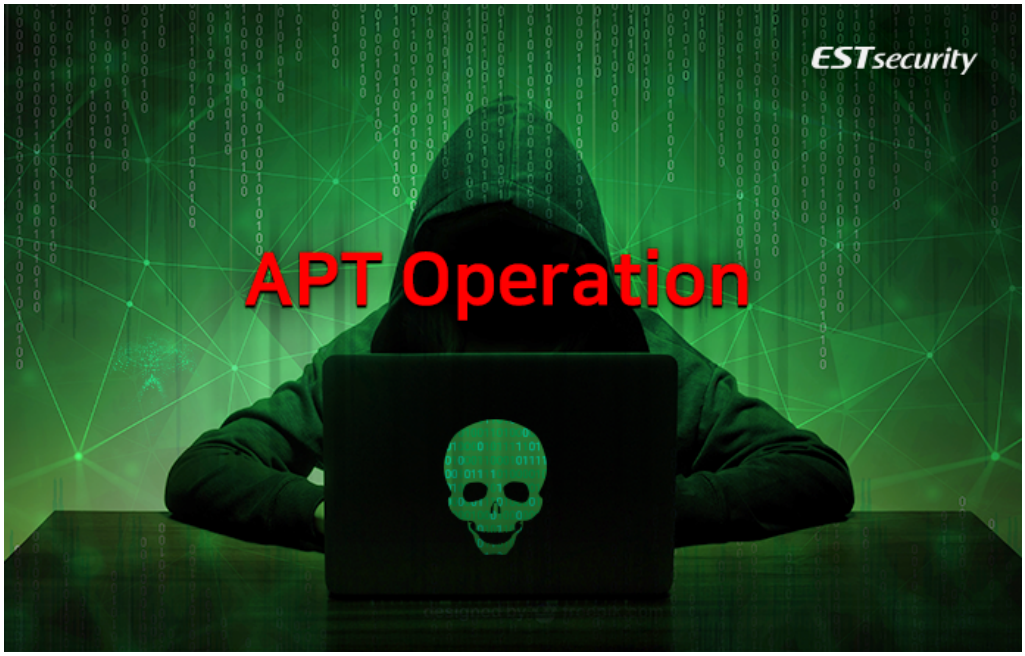
이스트시큐리티 기업 | 공지사항 | 라자루스(Lazarus), 소명자료요구서로 위장한 '무비 코인' 캠페인 지속

estsecurity.com/enterprise/security-center/notice/view/2096

라자루스(Lazarus), 소명자료요구서로 위장한 '무비 코인' 캠페인 지속

보안공지 2019-08-20



2019년 08월 13일 제작된 신규 악성 HWP 문서가 발견되었는데, 이번에는 국세청 관련 문서처럼 사칭한 공격이었습니다.

해당 악성코드를 조사해 본 결과, 지난 6월부터 7월까지 국내에서 지속적으로 발견되고 있는 '무비 코인(Movie Coin)' 시리즈로 분석되었습니다.

제목	마지막 저장시간 (UTC)	마지막 저장자	MD5
별지 제172호 서식	2019-08-13 02:32:05	User	7bece42a704800a6686cad43d3f5ee62

	Last Saved By	Revision Number	Last saved Time
에어컨 유지보수 특수조건.hwp	USER	8, 0, 0, 466 WIN32LEWindows_7	2019-07-02 10:14:58
20190626_현장프로젝트1 결과발표(4조).hwp	USER	8, 0, 0, 466 WIN32LEWindows_7	2019-06-26 10:16:16
Final(1-5).hwp	USER	8, 0, 0, 466 WIN32LEWindows_7	2019-07-23 15:48:15
중고품매각 공고문_19년 7차.hwp	USER	8, 0, 0, 466 WIN32LEWindows_7	2019-07-12 08:13:19
차트 4-5.hwp	USER	8, 0, 0, 466 WIN32LEWindows_7	2019-07-23 15:47:56
제북인 경찰대학 변형 문제 1회.hwp	USER	8, 0, 0, 466 WIN32LEWindows_7	2019-07-17 09:57:54
시스템 포팅 계약서(수정).hwp	USER	8, 0, 0, 466 WIN32LEWindows_7	2019-07-12 07:52:16
Last 1~5.hwp	USER	8, 0, 0, 466 WIN32LEWindows_7	2019-07-23 15:48:32
제북인 경찰대학 예상 문제 3회.hwp	USER	8, 0, 0, 466 WIN32LEWindows_7	2019-07-17 09:59:59
회장님 개명.hwp	USER	8, 0, 0, 466 WIN32LEWindows_7	2019-07-12 07:49:53
투자계약서_20190619.hwp	USER	8, 0, 0, 466 WIN32LEWindows_7	2019-06-18 23:56:17
(필수)외주직원 신상명세서.hwp	USER	8, 0, 0, 466 WIN32LEWindows_7	2019-07-12 07:50:52

라자루스(Lazarus) APT 그룹의 오퍼레이션 '무비 코인' 시리즈 관련 글은 아래와 같고, 지난 6월부터 8월까지 지속적인 활동이 포착되고 있습니다. 이번까지 총 7번째 리포팅이 진행되고 있습니다.

▶ 전방위 '무비 코인' APT 작전을 수행하는 Lazarus 그룹 위협 증대 (2019. 07. 23)

▶ 암호화폐 거래소 회원 겨냥한 무비코인 작전 지속… 배후에 '라자루스' 조직 (2019. 07. 19)

▶ 라자루스(Lazarus) APT 그룹, 신상명세서 문서로 위장한 공격 수행 (2019. 07. 15)

▶ 라자루스, 시스템 포팅 명세서 사칭한 APT작전 '무비 코인' 으로 재등장 (2019. 07. 12)

▶ 암호화폐 거래자를 노린 Lazarus APT 공격 가속화 (2019. 07. 02)

▶ 라자루스(Lazarus) APT 그룹, 암호화폐 투자계약서 사칭 무비 코인 작전 (2019. 06. 20)

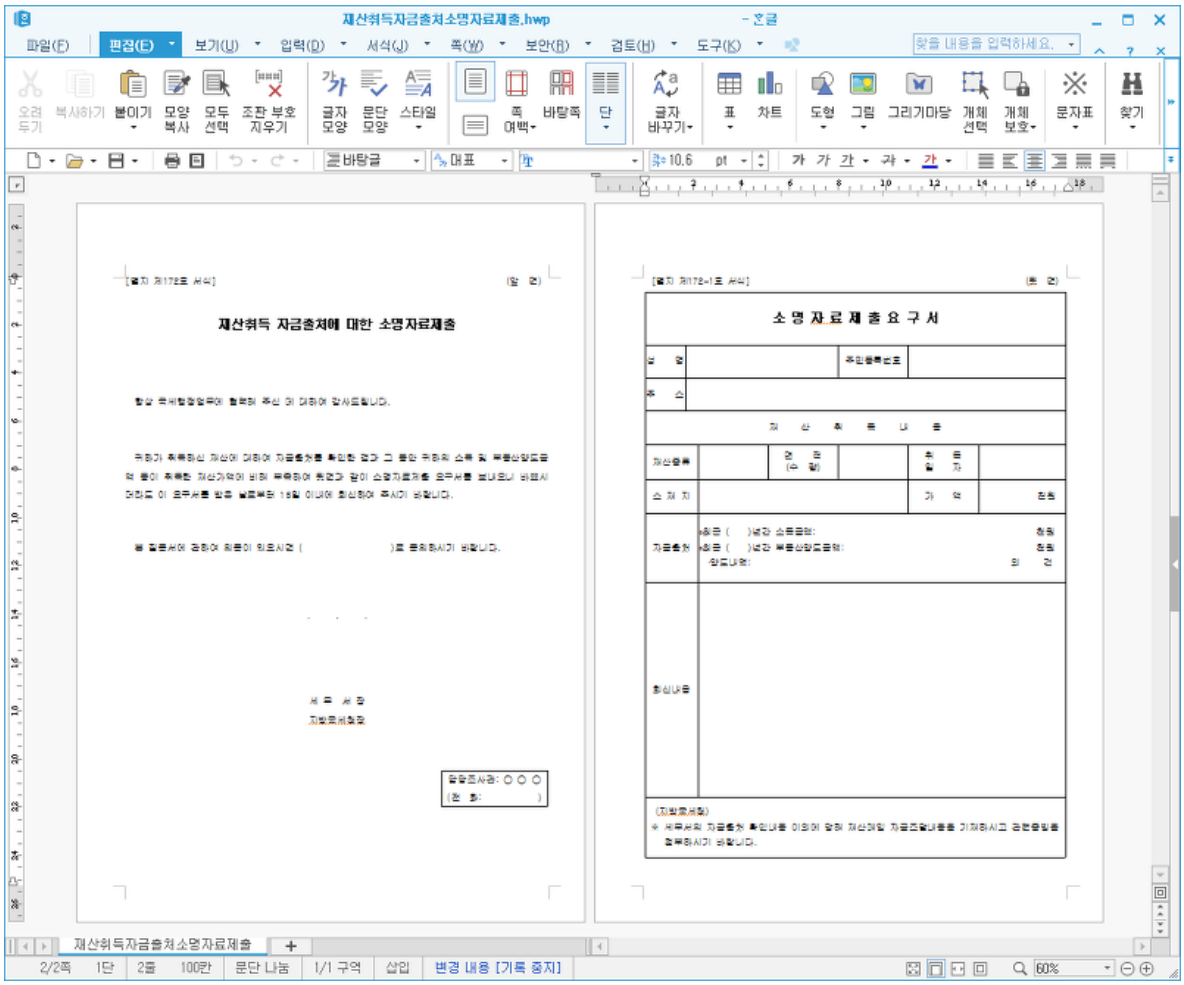
오퍼레이션 '무비 코인'의 경우, 위협배후에 대표적 정부후원 해킹조직인 '라자루스(Lazarus)' 그룹이 존재하는 것으로 알려져 있고, 국내 유명 암호화폐 거래소에 가입되어 있던 회원들이 주요 공격 대상에 포함되어 있습니다.

■ 라자루스 APT 조직, 사이버공격을 통한 금전적 수익시도 지속적 수행

이번 공격에 사용된 악성 HWP 문서는 기존과 마찬가지로 마지막 저장 계정이 'User'이며, 동일한 포스트스크립트(PostScript) 취약점을 활용했습니다.

그리고 인터넷에 공개되어 있는 실제 공문서 양식(재산취득 자금출처에 대한 소명자료제출)에 악성스크립트를 삽입했습니다.

인터넷에 공개되어 있는 정상문서에는 아래와 같이 앞면과 뒷면 2장으로 구성되어 있지만, 악성문서에는 뒷면의 '소명자료제출요구서' 내용만 포함되어 있습니다.



[그림 1] 정상적인 소명자료제출요구서 문서화면

공격자는 실제 정상문서 내용을 도용해 악성코드를 삽입하여 공격에 활용하였습니다.

이번과 유사한 공격기법은 이미 지난 2017년 05월 '납세담보변경요구서' 등의 악성 HWP 파일이 다수 보고된 바 있고, 그 이후로도 변종 HWP 파일이 다양한 유형으로 공격이 수행되었습니다.

[그림 2] 실제 비트코인 거래자들에게 전송된 스피어 피싱 화면

특히, 한국의 특정 암호화폐 거래소 직원 및 회원들을 대상으로 집중적인 공격이 수행되었습니다.

아래는 2017년부터 2018년까지 발견됐던 유사 변종 사례 중 시간흐름으로 일부만 정리한 것입니다.

주로 HWP 취약점이 사용되지만, 공격 대상에 따라 XLS, DOC 매크로 기능을 활용한 방법도 사용되었습니다. 당시 악성 문서파일 제작자는 비슷한 컴퓨터 계정을 사용하였습니다.

주로 'jikpurid', 'David', 'Administrator', 'Tiger', 'User', 'alosha' 등이고, 최근에는 'User' 계정이 계속 쓰이고 있습니다.

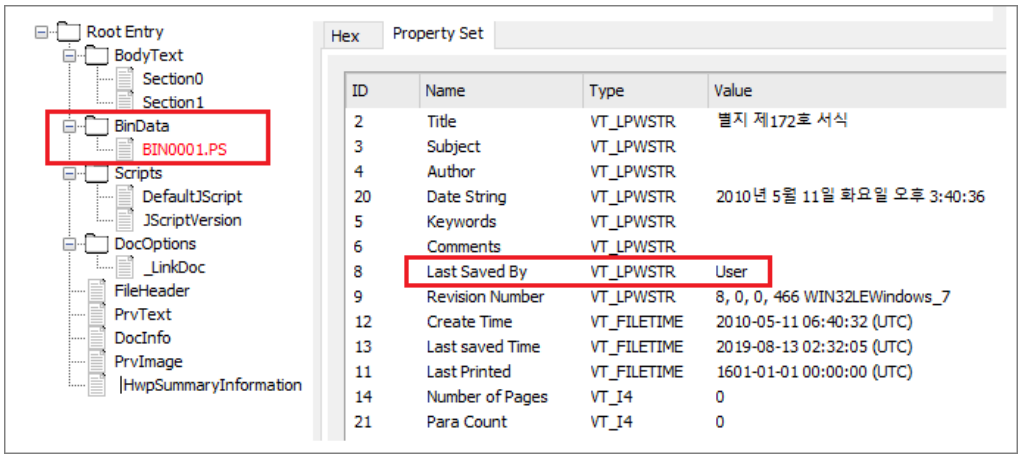
파일명	마지막 저장 시간 (UTC)	마지막 저장자	MD5
report.xls	2017-03-20 15:45:31	David (작성자 : jikpurid)	c272af488ff4c4af2941fd83b1484f33
이력서.hwp	2017-04-28 04:40:50	Administrator (작성자 : jikpurid)	2963055f30a0c04a4e7abf97b1d54faa
데이터.hwp	2017-05-02 04:48:11	jikpurid (작성자 : jikpurid)	0a355fb170b46479fee2796531a7f2ed
납세담보변경요구서.hwp	2017-05-16 00:49:41	Administrator	954de3d332e5de9889e8cc8936f7c83e

세무조사준비서류.hwp	2017-05-22 06:57:21	Administrator	f47ea4c8943f868d67cf69bb0770ab27
법인(개인)혐의거래보고내역.hwp	2017-05-22 10:07:15	jikpurid	f3c9b8f10a4982f898f755f0b352a53f
환전_해외송금_한도_및_제출서류.hwp	2017-05-29 04:05:14	Administrator	0f41c221b8ed10540e4f8ac4b125898e
국내 가상화폐의 유형별 현황 및 향후 전망.hwp	2017-06-12 06:45:54	Tiger	b84e781bbff0bbff63f3d88c6ce4d84e
이력서(김정희).hwp	2017-06-16 02:54:41	User (작성자 : jikpurid)	64054e877f48522f8a04a183843a9a39
입사지원서(곽정민).hwp	2017-06-16 02:58:01	User	5cf5bac15c27cc140cc482c722a81b0d
[가상화폐 법률] 국가별 가상화폐 허용 현황.hwp	2017-06-19 01:34:58	Tiger	be2d8ac855b605cce98bec3f8d334ce3
예금질권설정 서류안내(핀테크기업).hwp	2017-07-10 05:04:34	Administrator	a007249e09dd915d7c1c8072ad86b18a
비트코인_지갑주소_및_거래번호.hwp	2017-07-31 07:40:07	Administator	ec7ba18cc775a58647943e16d51d01ac
(대검)2017임시113호(마약류 매매대금 수익자 추정 지갑주소 164건).hwp	2017-08-04 00:57:10	Administrator	f420757270d0987148b950f2066bbbab
전산 및 비전산 자료 보존요청서.hwp	2017-08-10 05:23:20	User	1c0ee8e91704ca11cb4b9825541e8f7a
스트리미_조사사전예고통지 (1).hwp	2017-08-10 06:05:16	User	2cd28ee74910be7a023d10e3860eae5c
반성문.hwp	2017-08-16 10:32:25	alosha	d4a8acca0c0af629f600234d230ab0cf
유병록 입사지원서.hwp	2017-09-19 03:09:35	alosha	7de8b065e2587765fca5a163f958637d
한국블록체인협회_가입의향서.hwp	2017-09-21 04:47:53	alosha	0b93a989d776d627f9e079b03af0dc46
비트코인 관련 주요 범죄 수사결과.hwp	2017-10-13 03:18:57	alosha	ce3350131bbfca1a330dad62653a132d
[붙임]조사 당일 구비하여야 할 서류 1부.hwp	2017-10-17 08:30:00	김미숙	87c748f59f97dfb29b48079532b39e5c
김다은.hwp	2017-11-01 03:32:38	alosha	e50256b8e8496a030561f5ad6d9bda1e
김지예.hwp	2017-11-29 17:44:32	alosha	a687afc6a4540e5d44078aa933feecb6
정아경.hwp	2017-11-30 18:22:59	alosha	a6dd0124fb5cb054f1614f13f3f2fe48
(업체명)_가상화폐_거래소_정보보호_현황_자체점검표.hwp	2017-12-14 17:54:48	Administrator	8d7f9eef073b1971dfc1a231cdda9d30
가상화폐와 각국의 규제정책.hwp	2018-02-22 07:45:43	Administrator	e2cba0052fd8717fe33d5f8744cfd2a1

이학영_의원실_암호통화의_경제적_의미와_정책대응방향_토론회내지.hwp	2018-02-24 07:53:40	Administrator	a5892a400c85fd1a5053ca5caca742a7

■ 소명 자료 제출 요구서를 사칭한 코드 분석

소명 자료 제출 요구서로 위장한 악성 HWP 문서파일은 2019년 08월 13일 코드가 저장되었으며, 'BinData' 스트림에 'BIN0001.PS' 포스트스크립트(PostScript) 코드가 포함되어 있습니다.



[그림 3] 포스트스크립트와 HWP 문서파일 정보

포스트스크립트에는 다음과 같이 구성되어 있으며, 16바이트(39 C3 B2 70 05 85 3E 98 66 1C 8B BC 1B DD EA F8>)로 XOR 로직으로 암호화 되어 있습니다.

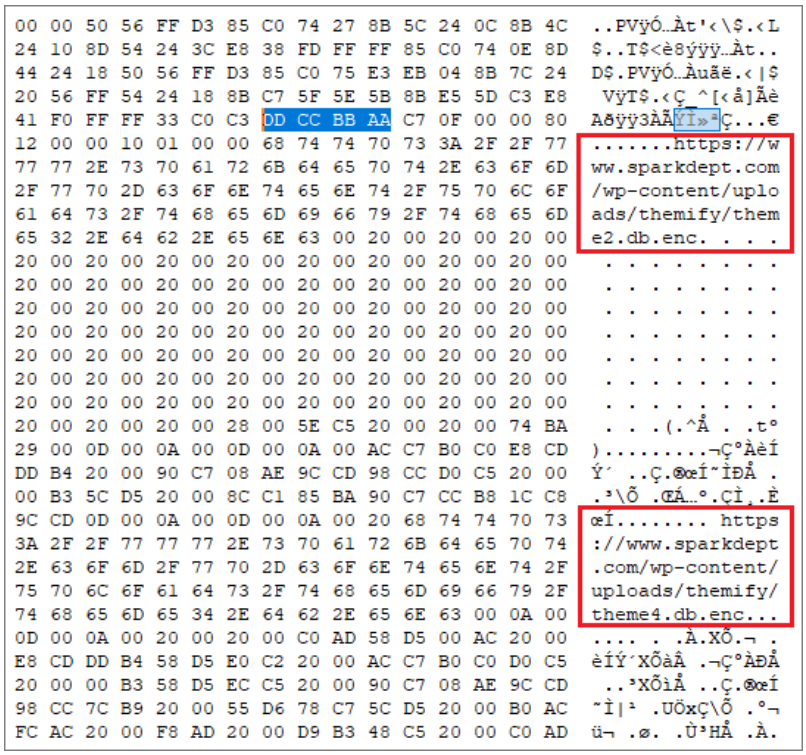
/Y101 <169A835034B31DDE205ACD9C7FB88CD8169A80505CB41EF9146EEAC53

-중간 생략-

5505CB409B83F2DBB8C3BECDCDB00FB921161E11EC15F28ABE52AEACAA10BE3835062E04AB80570E4CF7EBB83945CC9> def /Y102 <39C3B27005853E98661C8BBC1BDDEAF8> def 0 1 Y101 length 1 sub {/Y18 exch def Y102 Y18 15 and get Y101 Y18 get xor Y101 exch Y18 exch put} for Y101 cvx exec

복호화가 진행되면 2번째 포스트스크립트(PostScript) 코드가 나타나게 되며, 내부에 쉘코드(Shellcode) 로드를 수행하게 됩니다.

쉘코드 명령에 의해 특정 웹 서버 주소로 연결을 시도하게 되며, 감염된 윈도우즈 시스템에 따라 32비트용, 64비트용 암호화된 악성코드가 선택됩니다.



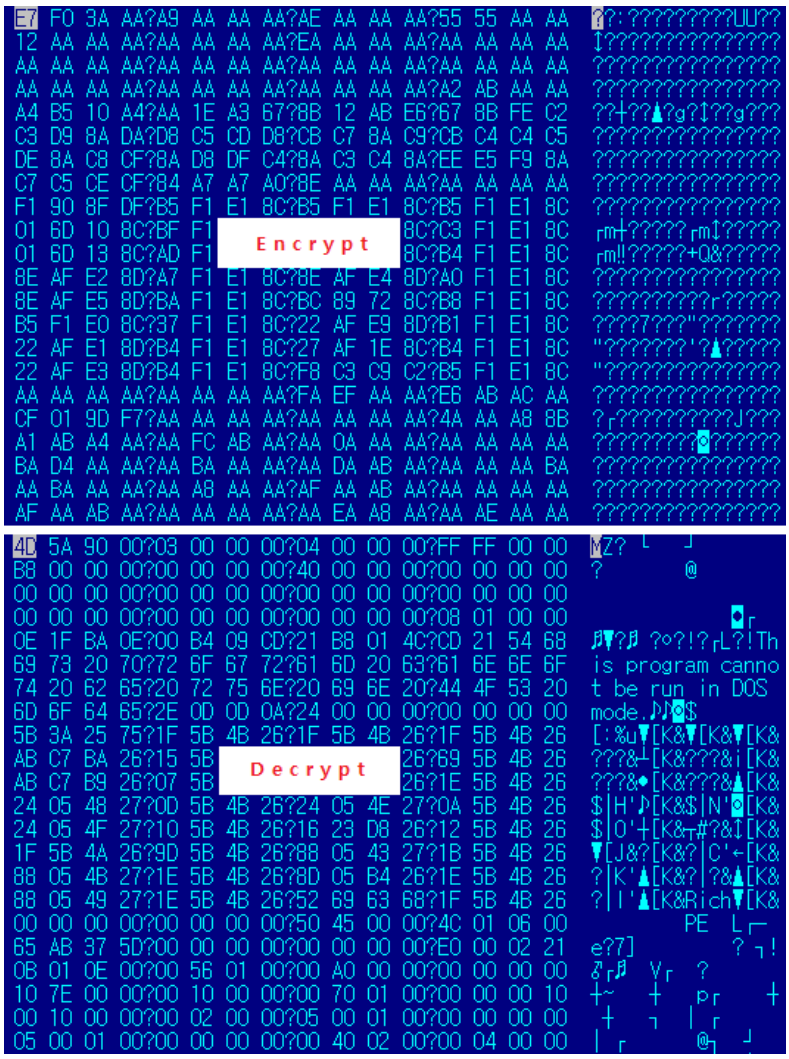
[그림 4] 쉘코드에 포함되어 있는 C2 서버 화면

- https://www.sparkdept[.]com/wp-content/uploads/themify/theme2.db.enc (32비트)

- https://www.sparkdept[.]com/wp-content/uploads/themify/theme4.db.enc (64비트)

공격자가 만든 파일명 'theme2.db.enc', 'theme4.db.enc' 확장자에도 마치 암호화(Encrypt)된 것을 의미하는 단어가 지정되어 있습니다.

각각의 파일은 0xAA 키로 1바이트씩 XOR 로직으로 암호화되어 있으며, 복호화를 거치면 아래화면과 같이 악성 DLL 파일이 생성됩니다.



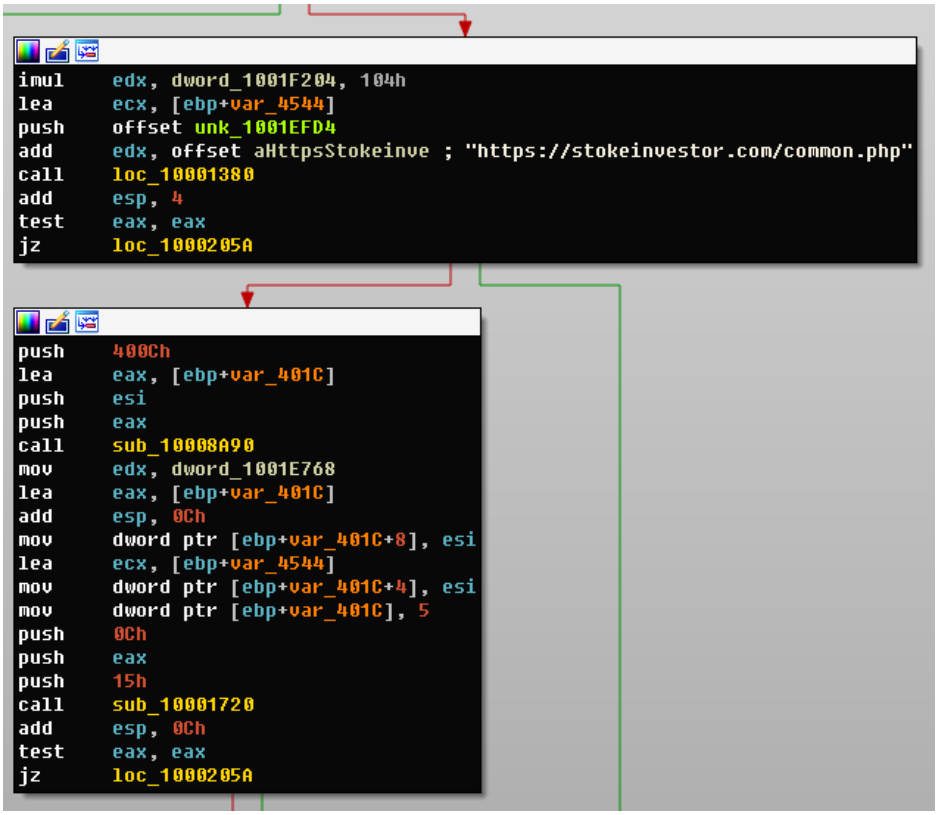
[그림 5] 최종 페이로드 파일 암/복호화 비교 화면

최종 악성모듈은 3개의 명령제어(C2) 서버로 통신을 시도하며, 감염된 컴퓨터의 정보를 유출시도하고, 공격자의 추가 명령을 대기하게 됩니다.

- https://stokeinvestor[.]com/common.php

- https://growthincone[.]com/board.php

- https://inverstingpurpose[.]com/head.php



[그림 6] C2 접속 코드 화면

ESRC는 이 3개의 C2 도메인을 조사하는 과정 중에 흥미로운 점을 발견했습니다. C2 서버 3곳 모두 거의 동일한 시점에 동일한 곳에서 등록되었다는 것입니다.

이런 점을 유추해 볼 때 공격자가 직접 C2 서버를 등록하고 구축해 사용했을 가능성도 배제할 수 없습니다. 최근까지 워드 프레스 기반의 웹 서버가 C2 호스트로 악용되었습니다.

growthincone.com	stokeinvestor.com	inverstingpurpose.com
Registry Domain ID: 2395886348_DOMAIN_COM-VRSN	Registry Domain ID: 2395886352_DOMAIN_COM-VRSN	Registry Domain ID: 2395886354_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.namecheap.com	Registrar WHOIS Server: whois.namecheap.com	Registrar WHOIS Server: whois.namecheap.com
Registrar URL: http://www.namecheap.com	Registrar URL: http://www.namecheap.com	Registrar URL: http://www.namecheap.com
Updated Date: 2019-05-28T08:43:12.00Z	Updated Date: 2019-05-28T08:43:14.00Z	Updated Date: 2019-05-28T08:43:15.00Z
Creation Date: 2019-05-28T08:43:12.00Z	Creation Date: 2019-05-28T08:43:14.00Z	Creation Date: 2019-05-28T08:43:15.00Z
Registrar Registration Expiration Date: 2020-05-28T08:43:12.00Z	Registrar Registration Expiration Date: 2020-05-28T08:43:14.00Z	Registrar Registration Expiration Date: 2020-05-28T08:43:15.00Z
Registrar: NAMECHEAP INC	Registrar: NAMECHEAP INC	Registrar: NAMECHEAP INC
Registrar IANA ID: 1068	Registrar IANA ID: 1068	Registrar IANA ID: 1068

■ 결론

이처럼 최근 비트코인, 이더리움 등 암호화폐를 거래하는 이용자를 대상으로 한 꾸준한 APT 공격이 수행되고 있습니다.

특히, HWP 취약점을 이용한 스피어 피싱(Spear Phishing) 공격이 은밀하게 진행되고 있으므로, 사용중인 문서 소프트웨어를 반드시 최신 버전으로 업데이트하여야 하고, DOC, XLS 파일의 매크로 실행은 절대 허용하지 않는 것이 좋겠습니다.

라자루스와 관련된 APT 공격 사례들은 아래 포스팅을 참고해 주시기 바라며, 해당 악성코드들은 알약에 치료 기능이 추가되고 있습니다.

▶ 라자루스 APT, 국내 보안업체의 유효한 디지털서명을 탑재한 악성코드 주의! (2019. 07. 30)

▶ 라자루스(Lazarus) APT 조직, 텔레그램 메신저로 '진실겜.xls' 악성 파일 공격 (2019. 06. 27)

▶ 라자루스(Lazarus) APT, 유령 꼭두각시(Operation Ghost Puppet) (2018. 09. 20)

▶ 국가기반 APT 그룹 '오퍼레이션 스타 크루저(Operation Star Cruiser)' 수행 (2018. 04. 26)

▶ '오퍼레이션 배틀 크루저' 다양한 취약점으로 국내외 APT 공격 지속 (2018. 04. 11)

목록