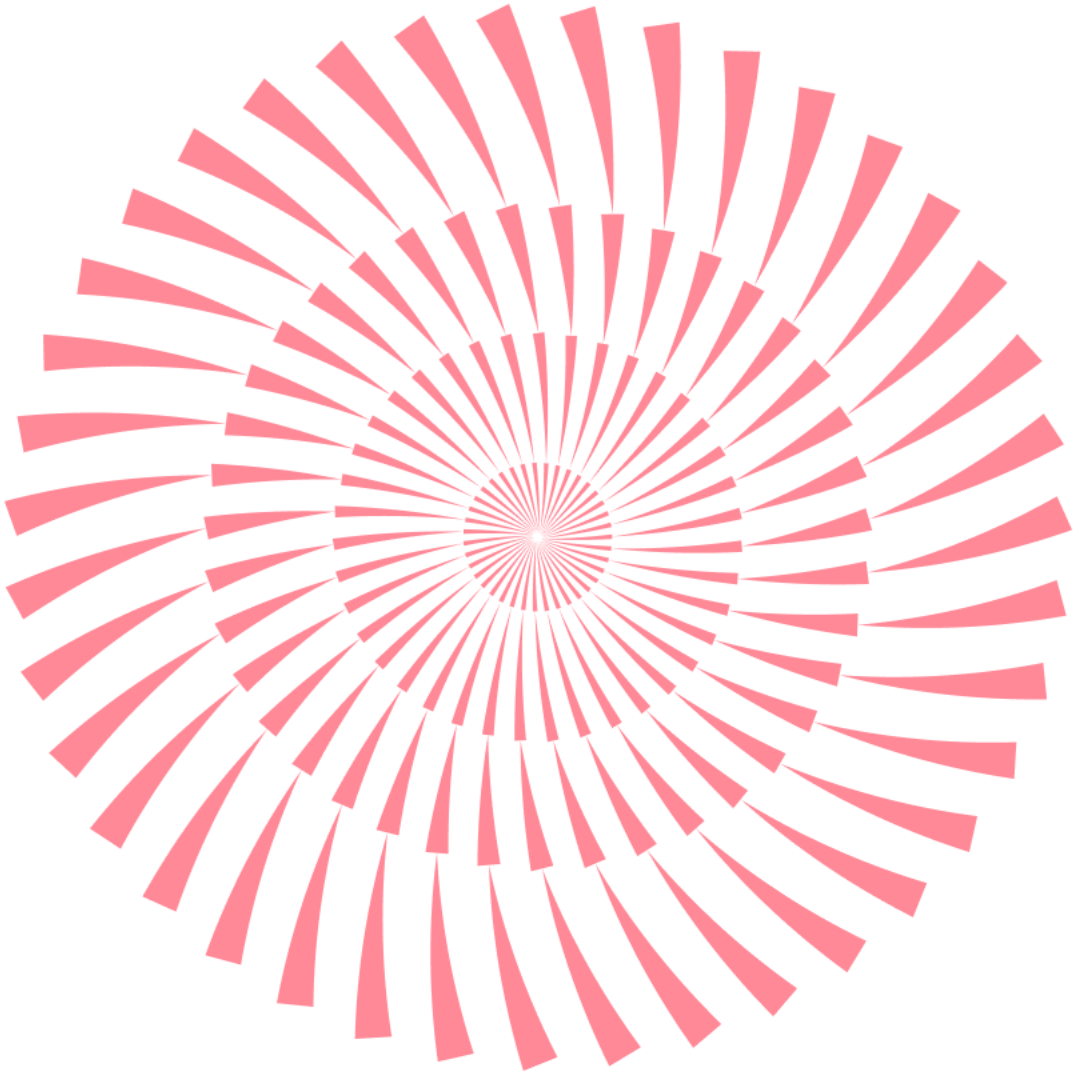
No.175 | 2024.4

ESRC 보안동향보고서

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



EST SECURITY

ESRC 보안동향보고서

CONTENTS

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

북한의 지원을 받는 해킹 조직의 공격이 여전히 지속되고 있습니다.

지난해 사법부 전산망 해킹과 관련한 조사 결과가 발표되었는데, 사법부 전산망 해킹으로 인해 약 600GB 의 자료들이 유출되었으며, 최초 알려진 서울중앙지방법원 스캔서버 외에 인터넷 가상화시스템 계정을 관리하는 AD(Active Directory)서버와 가상화웹서버, 가상 PC 등이 해킹을 당했다고 밝혔습니다.

다목적실용위성과 공공위성인 차세대중형위성의 운영을 책임지고 있는 국가위성운영센터도 해킹 당한 것이 뒤늦게 확인되었는데, 이 해킹사건들의 배후에는 모두 북한이 있는 것으로 추정되고 있습니다.

LockBit 랜섬웨어가 돌아왔습니다.

24 년 2 월 20 일, 10 개국의 법 집행 기관이 합동작전을 통하여 LockBit 의 서비스를 압수하였습니다. Operation Cronos 라고 명명된 이 작전을 통하여 LockBit 의 소스코드, 1000 개 이상의 암호 해독키, 도메인을 포함한 다양한 정보들을 압수하였고, 이로 인해 LockBit 은 서비스 중단 이라는 큰 타격을 입었습니다.

하지만 2 월 24 일 LockBit 은 이에 굴하지 않고 새 다크웹 개설과 더불어 범죄를 지속하겠다는 성명을 내며 재건의 의지를 내비쳤으며, 3 월 21 일에는 LockBit 은 정보 탈취 기업과 몸값을 낼 기한도 함께 표기 된 새로운 다크웹을 구축하여 공개하기도 했습니다. 하지만 LockBit 조직이 성공적으로 복귀할 수 있을지는 지켜봐야겠습니다.

23 년 3 월 14 일 공포된 개인정보보호법의 일부 규정이 3 월 15 일부터 본격 시행되었습니다.

시행된 개정법에는 인공지능(AI) 확산에 따른 자동화된 결정에 대해 정보주체인 국민의 권리를 신설하고, 개인정보를 보다 전문적으로 보호하기 위해 대량 또는 민감한 개인정보를 처리하는 기업, 공공기관 등의 개인정보 보호책임자(CPO) 자격 요건을 강화하는 내용이 포함된 만큼, 개인정보보호 업무 담당자분들은 개정된 내용에 대해 꼼꼼히 살펴봐야겠습니다.

KISA 가 정보통신망법 안내서 개정본을 발간하였습니다.

이번 개정본에는 불법스팸 전송자 처벌 강화 및 통신사의 전송 방지 책임성 강화를 위한 처벌 상향, 이용자 수신 동의 및 전송자 금지 행위 관련 해석이 모호한 단어를 명시적으로 단어로 변경 등의 내용이 담겼으며, 법 개정과는 별도로 기존 안내서 상의 '수신 동의 여부 확인'과 관련한 설명을 보완하여 전송자의 이해를 높이고자 노력하였습니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

감염 악성코드 Top 15 는 사용자 PC 에서 탐지된 악성코드를 기반으로 산출한 통계입니다.

2024 년 3 월에는 새롭게 탐지된 Win32.Generic.5420 가 1 위를 차지하였습니다.
그 밖에도 Win32.Generic.5420, Exploit.CVE-2010-2568.Gen, Gen:Variant.Tedy.508314, Gen:Variant.Razy.613998 , Gen:Variant.Lazy.20522, Gen:Variant.Ulise.144799 , Trojan.GenericKD.71855533, Trojan.DDoS.Nitol.gen, Application.Hacktool.BBJ, Trojan.Acad.Bursted.AK, Trojan.Agent.PureLogs, Spyware.Infostealer.Bladabindi , 등 다수의 새로운 탐지명이 순위권에 진입하였으며, OS/SW 불법인증툴 관련 탐지명 Misc.HackTool. AutoKMS 툴이 5 단계 상승했습니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	NEW	Win32.Generic.5420	Virus	130,450
2	NEW	Exploit.CVE-2010-2568.Gen	ETC	89,105
3	NEW	Gen:Variant.Tedy.508314	ETC	72,679
4	NEW	Gen:Variant.Razy.613998	ETC	63,151
5	↑5	Misc.HackTool.AutoKMS	ETC	43,719
6	NEW	Gen:Variant.Lazy.20522	ETC	40,486
7	↑6	Backdoor.Generic.792814	Backdoor	32,405
8	NEW	Gen:Variant.Ulise.144799	ETC	30,686
9	NEW	Trojan.GenericKD.71855533	Trojan	28,641
10	NEW	Trojan.DDoS.Nitol.gen	Trojan	27,711
11	NEW	Application.Hacktool.BBJ	ETC	26,976
12	NEW	Trojan.Acad.Bursted.AK	Trojan	26,382
13	NEW	Trojan.Agent.PureLogs	Trojan	22,221
14	↑1	Trojan.HTML.Ramnit.A	Trojan	21,958
15	NEW	Spyware.Infostealer.Bladabindi	Spyware	19,295

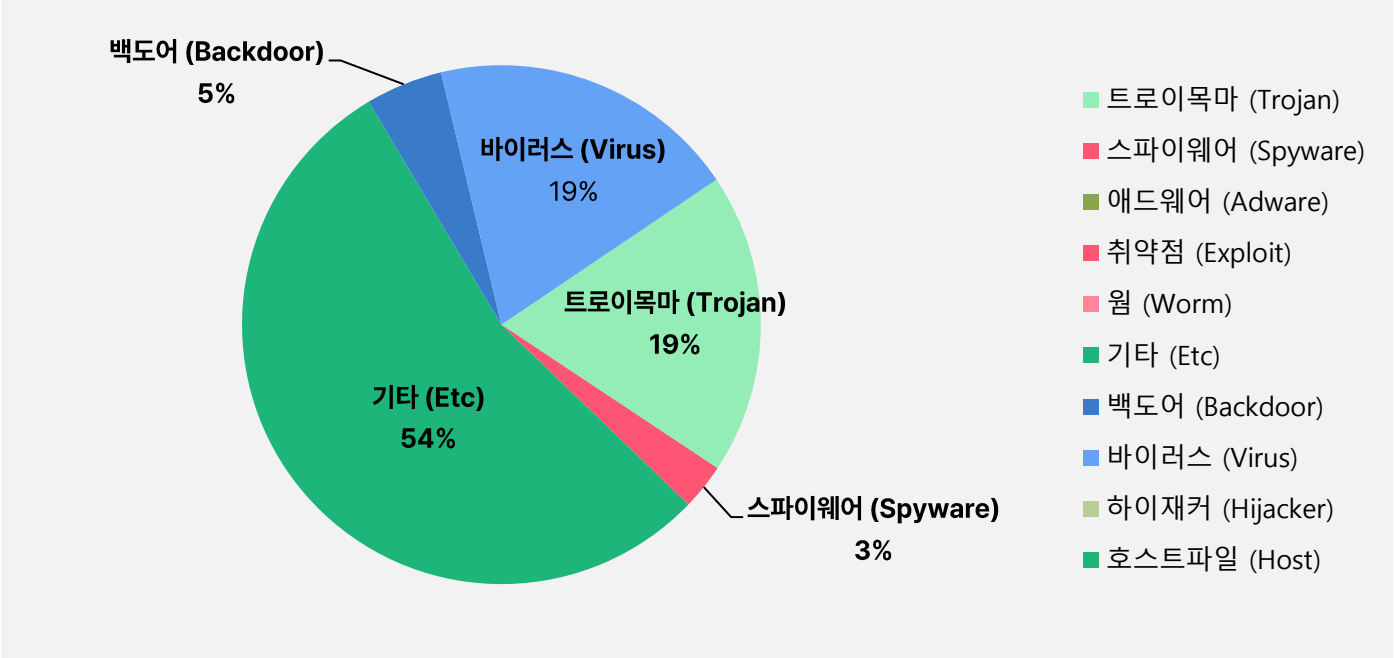
*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2024 년 3 월 1 일 ~ 2024 년 3 월 31 일

악성코드 유형별 비율

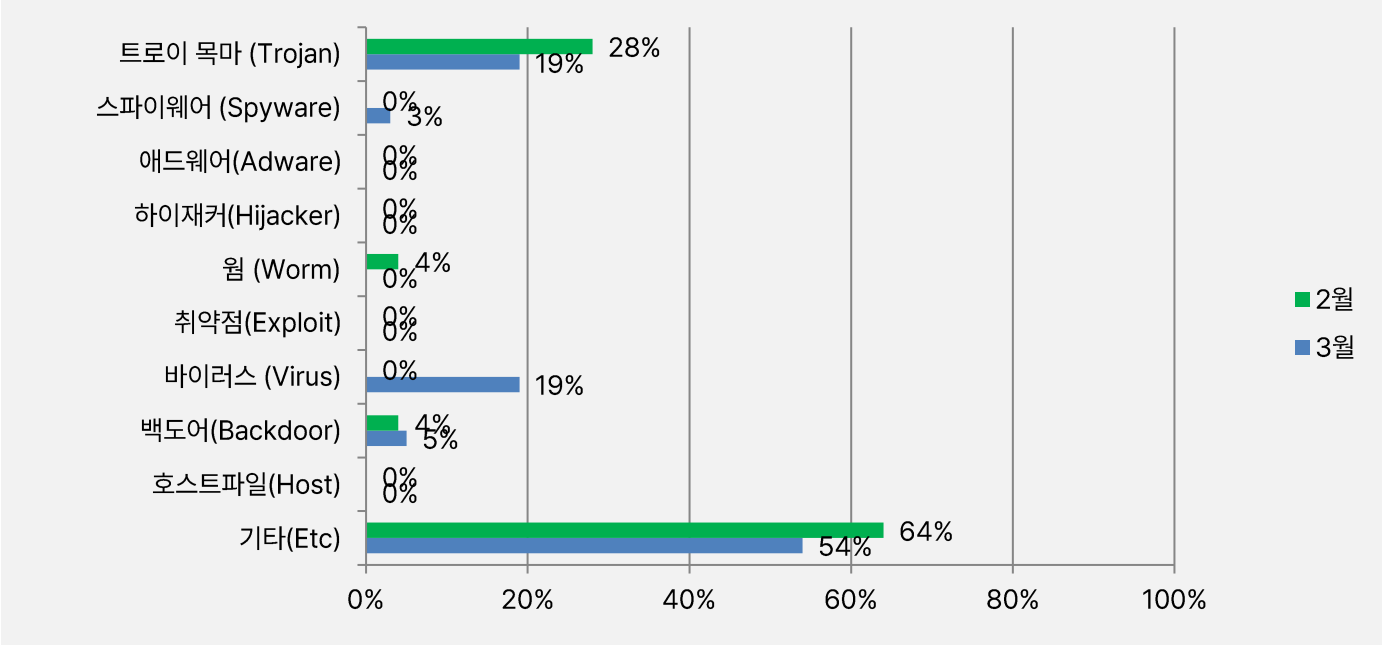
악성코드 유형별 비율에서 기타(ETC) 유형이 54%로 가장 높은 비율로 탐지되었으며, 그 다음으로 트로이목마(Trojan) 유형과 바이러스(Virus)가 19%, 백도어(Backdoor), 스파이웨어(Spyware) 유형이 각각 5%, 3%로 확인되었습니다.

2024 년 2 월과 비교하여 전체 감염 건수는 77% 가량 감소하였습니다.



카테고리별 악성코드 비율 전월 비교

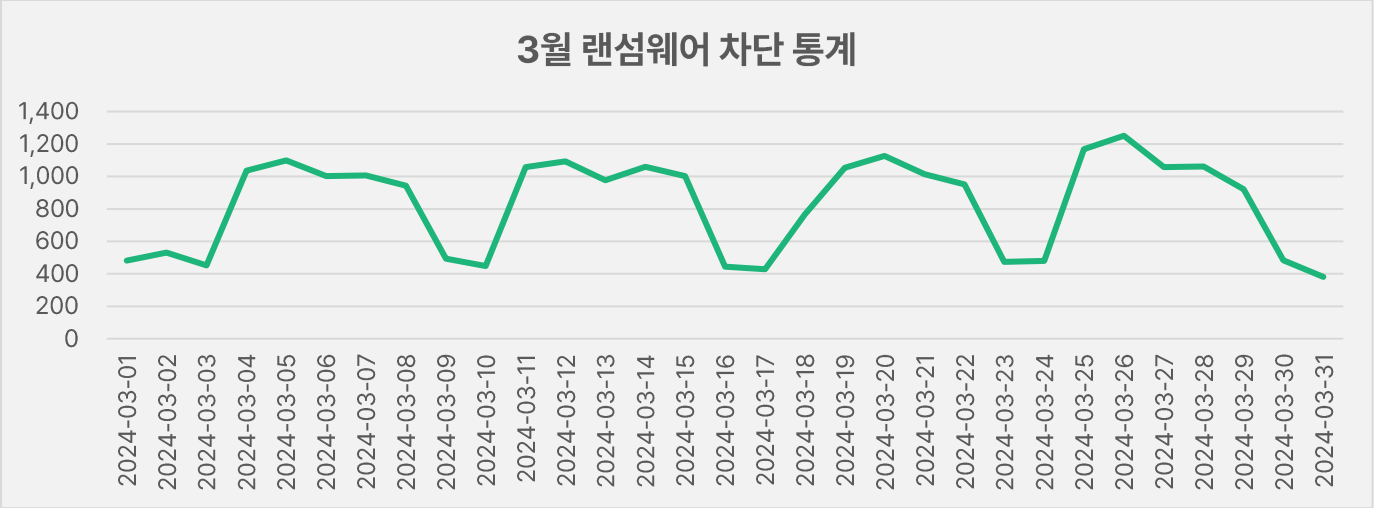
2024 년 3 월에는 지난 2 월과 비교하여 트로이목마(Trojan) 유형이 19%, 기타(ETC) 유형이 54%로 감소하였으며, 바이러스(Virus) 유형과 스파이웨어(Spyware)가 새로 등장해 각각 19%, 3%를 차지하였습니다. 백도어(Bakcdoor) 유형이 5% 소폭 증가하였습니다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

3 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 3 월 1 일부터 3 월 31 일까지 총 25,743 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 3 월 한 달간 총 8,021,258 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 2 월 한 달간 확인되었던 7,826,854 건의 악성코드 경유지/유포지 URL 수에 비해 약 2.48% 가량 증가한 수치입니다. 악성코드 경유지/유포지 URL 의 경우, 항상 고정적인 URL 만 모니터링하는 것이 아닌 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.

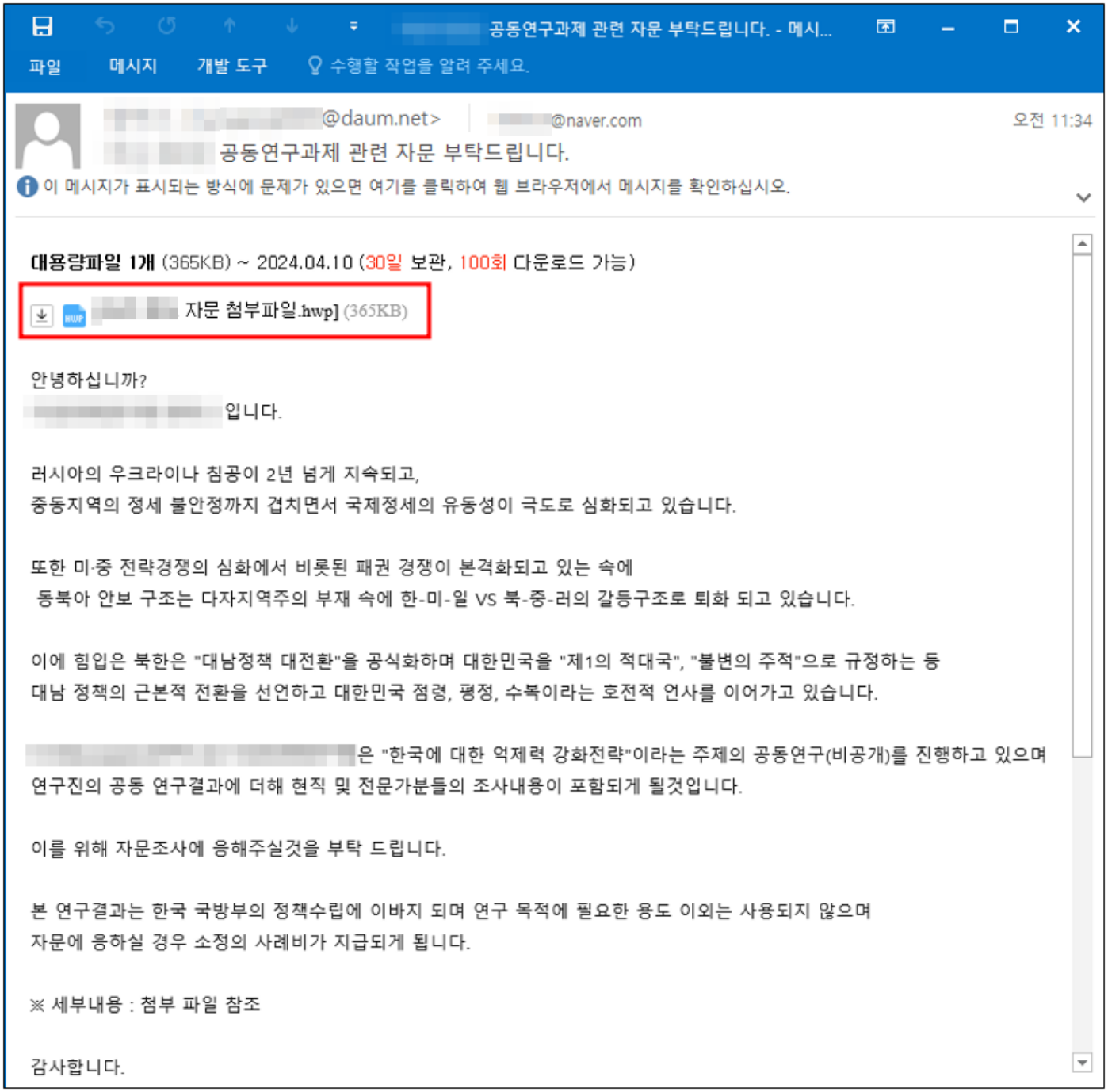
2

최신 보안 동향

북 킴수키(Kimsuky) 조직의 정책 자문 위장 스피어 피싱 주의!

국내 외교안보분야의 민간 정책연구원을 사칭하여, 실제 국방 관련 국가기관에 소속되어 있는 특정인을 타깃으로 한 스피어피싱 공격이 발견되어 주의가 필요합니다.

이번 피싱 메일은 'OO-OOOO 공동연구과제 관련 자문 부탁드립니다.' 라는 제목으로 유포되었고, 대용량파일 'OO-OO 자문 첨부파일.hwp'의 다운로드를 유도하고 있습니다.



[그림 1] 민간 정책연구원 사칭 메일

해당 첨부파일의 다운로드 버튼을 클릭하면 아래와 같이 네이버 로그인을 위장한 피싱 사이트로 연결되고, 여기에 입력한 계정 정보는 공격자의 서버로 전송됩니다.

[그림 2] 네이버 로그인으로 위장한 피싱 페이지

Body

Name	Value
id	ghdrlfehd
pw	1q2w3e4r

[그림 3] 공격자의 서버로 전송되는 계정 정보

여기까지는 일반적인 피싱이라고 생각할 수 있지만 메일의 첨부파일로 위장한 '[OO-OO 자문 첨부파일.hwp]' 부분의 코드를 살펴보면, a 태그를 이용한 단순 링크가 아닌 form 태그를 사용하였고 hidden 타입으로 된 input 태그에 base64 로 인코딩된 문자열이 확인됩니다.

이를 풀어 보면 "[피싱대상 ID]**[실제첨부파일 url]"의 형태로 구성된 것을 볼 수 있고, 실제 공격 타깃이 계정 정보를 입력해 정상적으로 로그인하였다면 공격자에게 계정정보가 넘어가고, 피해자는 정상 HWP(OO-OO 자문 첨부파일.hwp) 첨부파일을 다운로드 받아 계정정보 탈취 사실을 눈치채지 못하였을 것으로 보입니다.

[그림 4] 악성 사이트로 링크된 스크립트

```
ftstblue**https://attach.mail.daum.net/bigfile/v1/urls/d/J8GlYRtO-JymJaVe98UOikfj-Qo/HVOueYVOw4C-LGO5zkTSsg
```

[그림 5] 숨겨진 base64 문자열 디코딩 내용

㈜이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

www.estsecurity.com