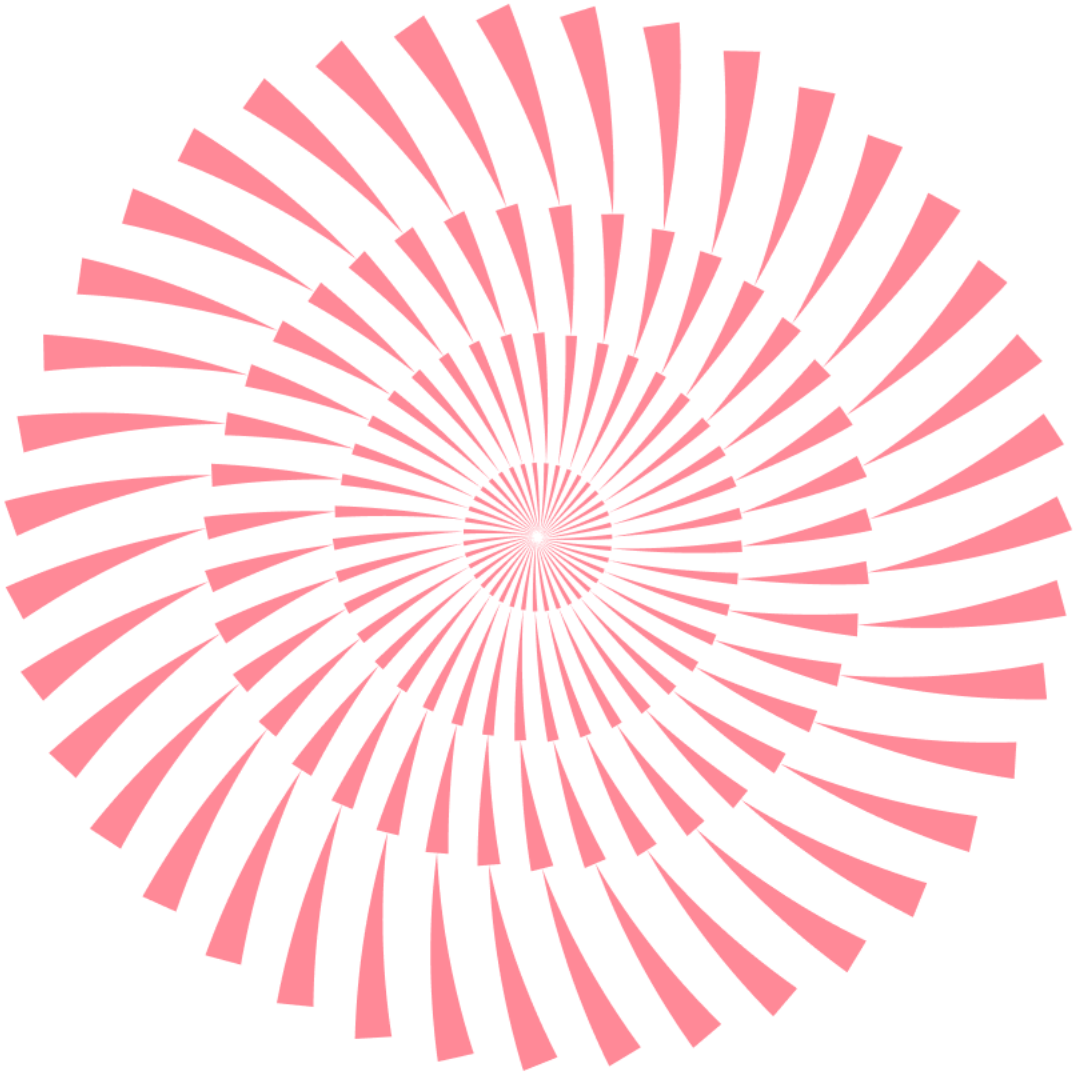
No.177 | 2024.6

ESRC 보안동향보고서

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



Copyright©2024 ESTsecurity Corp. All rights reserved.

EST SECURITY

ESRC 보안동향보고서

CONTENTS

1 악성코드 통계 및 분석 01-07

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

2 최신 보안 동향 08-12

국정원을 사칭하여 유포중인 이메일 주의!

1

악성코드 통계 및 분석

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

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

1. 악성코드 동향

정부 및 공공기관을 사칭한 범죄가 증가하고 있습니다.

4 월 중순부터 유포되기 시작한 정보 및 공공기관 사칭 악성 메일들은 5 월에도 국세청이나 한국인터넷 진흥원을 사칭한 형태로 지속적으로 발견되고 있으며, 사용자들을 속이기 위하여 발신자 정보를 실제 정부 24 콜센터 대표번호인 1588-2188 로 조작하여 발송한 스미싱 문자들이 발견되기도 했습니다.

이러한 상황의 심각성을 느낀 한국인터넷진흥원은 '정부기관 사칭 피싱메일 주의 및 도메인 보안설정 권고', '기업 문자발송 시스템 및 계정 해킹을 통한 스팸문자 발송 증가에 따른 주의 필요' 공지를 통하여 사용자들의 주의를 당부하였습니다.

북한 해킹 공격 조직의 공격이 국내외 적으로 지속되고 있습니다.

북한 해킹 조직의 공격으로 군 관계자 100 여명의 개인 이메일이 해킹 당했는데, 이 중에는 국방부 및 합동참모본부 고위급 인사가 다수 포함되어 있는 것으로 밝혀졌습니다. 앞서 북한 해킹 공격 조직은 최소 2 년간 법원 전산망에서 1TB 가 넘는 자료들을 탈취하였고, 국내 방산업체 10 여곳을 해킹한 사실이 밝혀지기도 했습니다.

연방수사국(FBI), 미국 국무부, 국가안보국(NSA)은 공동 권고문을 통해 킴수키 공격자들의 새로운 스피어피싱 기법을 공개하였습니다.

DMARC 정책은 도메인의 발신자 정책 프레임워크(SPF) 및 도메인키 식별 메일(DKIM) 레코드를 확인한 후 해당 이메일에 대해 스팸으로 표시하거나 받은 편지함으로 전달될 수 있도록 하는 정책인데, 킴수키는 DMARC 인증 정책이 미흡한 곳을 찾아내어 마치 합법적인 도메인에서 보낸 것처럼 스푸핑된 이메일을 보내 공격을 진행하였다고 밝히며, 이메일 보안강화를 권고하였습니다.

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2024 년 5 월에는 새롭게 탐지된 Gen:Variant.Lazy.266772 이 1 위를 차지하였습니다. 그 밖에도 Gen:Variant.Lazy.20522, Gen:Variant.Razy.241020, Win32.Gosys.B, Application.Hacktool.BBJ, Gen:Variant.Ulise.144799, Trojan.DDoS.Nitol.gen 등 다수의 새로운 탐지명이 순위권에 자리하였습니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	NEW	Gen:Variant.Lazy.266772	ETC	111,989
2	NEW	Trojan.Downloader.MSIL	Trojan	41,367
3	↑5	Misc.HackTool.AutoKMS	ETC	41,279
4	↑7	Backdoor.Generic.792814	Backdoor	40,867
5	NEW	Gen:Variant.Lazy.20522	ETC	30,935
6	NEW	Gen:Variant.Razy.241020	ETC	29,301
7	NEW	Win32.Gosys.B	Virus	27,146
8	NEW	Application.Hacktool.BBJ	ETC	26,670
9	NEW	Gen:Variant.Ulise.144799	ETC	25,448
10	NEW	Trojan.DDoS.Nitol.gen	Trojan	24,146
11	NEW	Trojan.Acad.Bursted.AK	Trojan	18,349
12	NEW	Misc.HackTool.KMSActivator	ETC	16,242
13	NEW	Win32.Neshta.A	ETC	14,171
14	NEW	Worm.ACAD.Bursted	Worm	12,740
15	NEW	Gen:Variant.Sirefef.2727	ETC	12,488

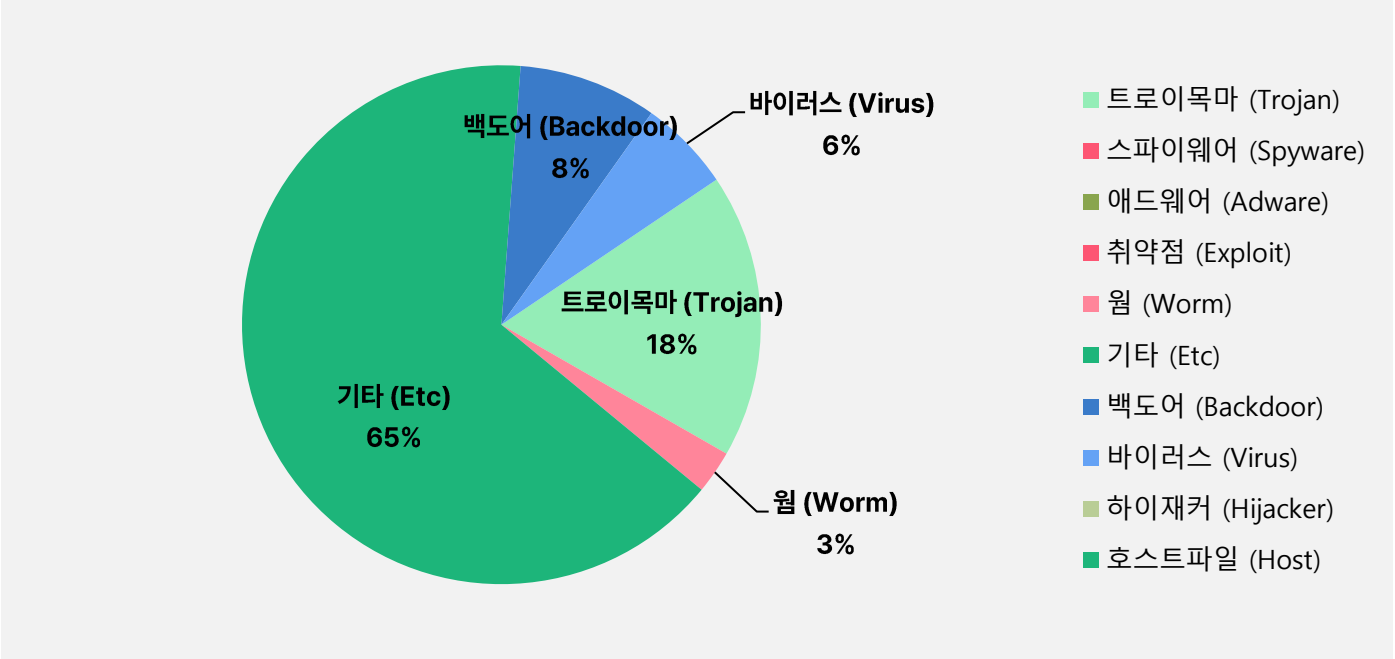
*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2024 년 5 월 1 일 ~ 2024 년 5 월 31 일

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

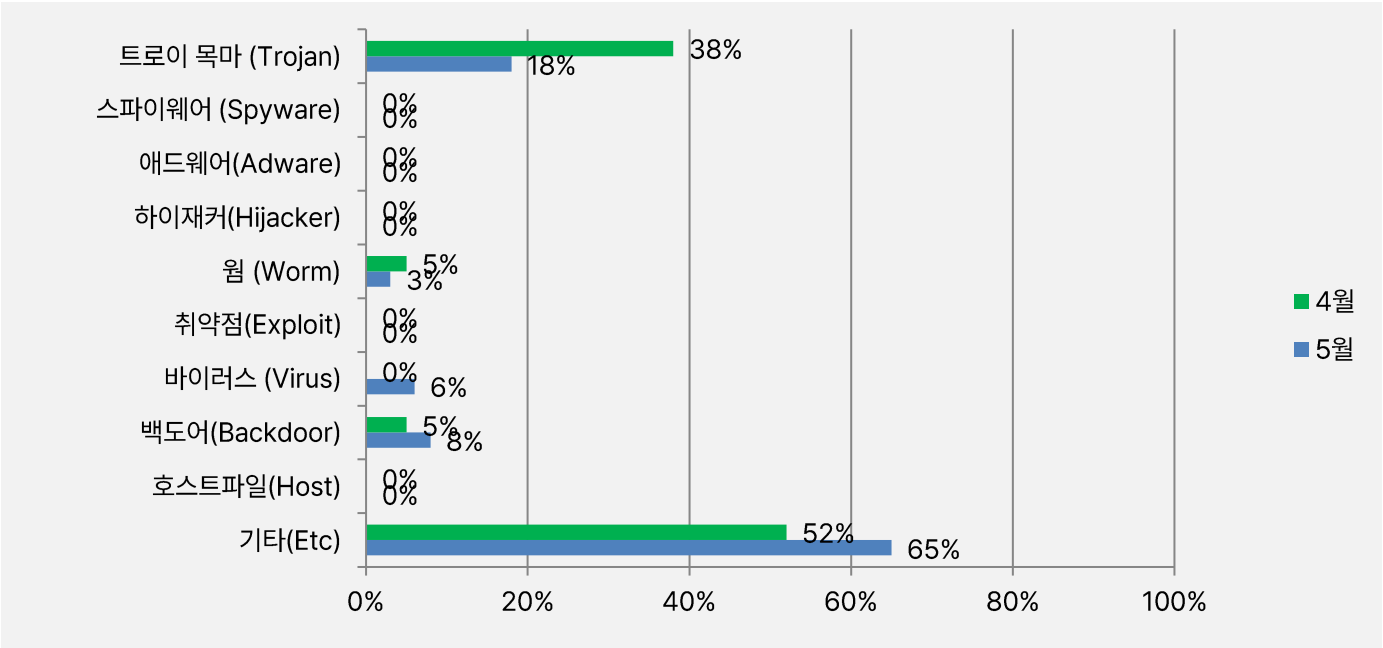
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 65%로 가장 높은 비율로 탐지되었으며, 그 다음으로 트로이목마(Trojan) 유형이 18%, 백도어(Backdoor) 8%, 바이러스(Virus) 6%, 웜 Worm) 유형이 3%로 확인되었습니다.



카테고리별 악성코드 비율 전월 비교

2024 년 5 월에는 지난 4 월과 비교하여 트로이목마(Trojan) 유형이 20% 대폭 감소하였고, 기타(ETC) 유형이 18% 증가하였습니다. 또한, 웜 (Worm) 유형이 2% 감소하였고, 백도어(Backdoor) 유형은 3% 증가하였습니다. 또한 바이러스(Virus)유형이 새로 등장하였습니다.

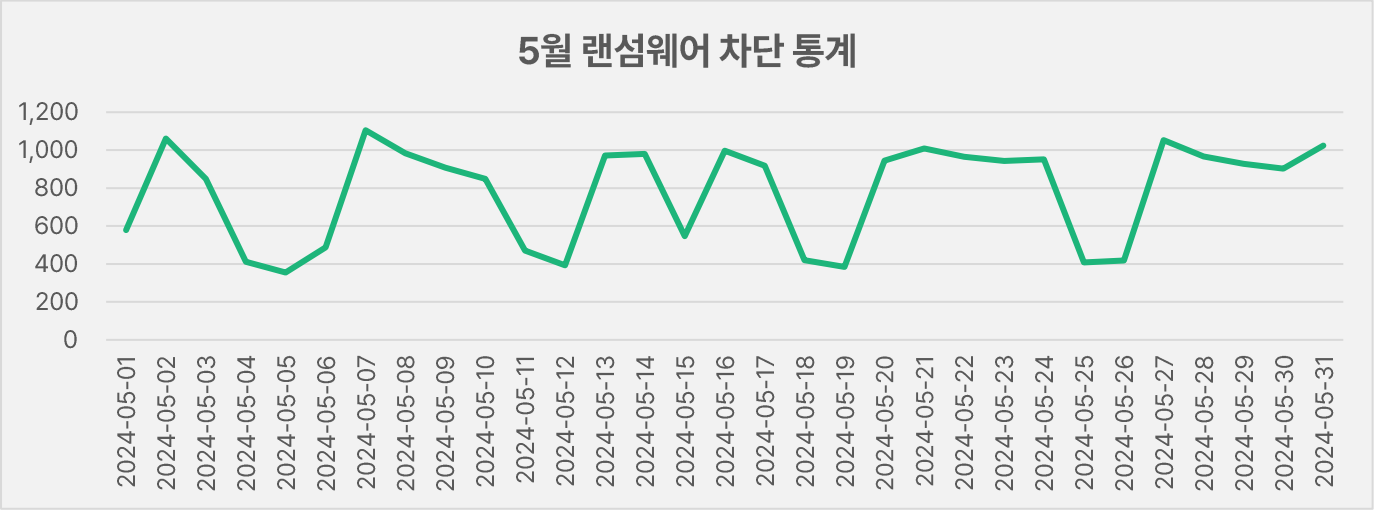


 Copyright©2024 ESTsecurity Corp. All rights reserved.

3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

5 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. 5 월 1 일부터 5 월 31 일까지 24,180 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 5 월 한 달간 총 8,053,634 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 4 월 한 달간 확인되었던 7,893,329 건의 악성코드 경유지/유포지 URL 수에 비해 약 2% 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.



ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

2

최신 보안 동향

ESTsecurity Copyright©2024 ESTsecurity Corp. All rights reserved.

국정원을 사칭하여 유포중인 이메일 주의!

지난달 국정원을 사칭한 피싱 메일이 발견되어 국정원 공지사항을 통해 안내가 되었으나 해당 피싱 메일이 지속적으로 유포되고 있는 것으로 확인되어 주의가 필요합니다.



[그림 1] 국정원 공지내용

해당 피싱 메일은 여전히 ‘ 경찰보고서’ 라는 제목으로 발신자명을 국가정보원으로 위장하여 발송되었으며, ‘국가정보원(한국).pdf’ 파일이 첨부되어 있습니다.

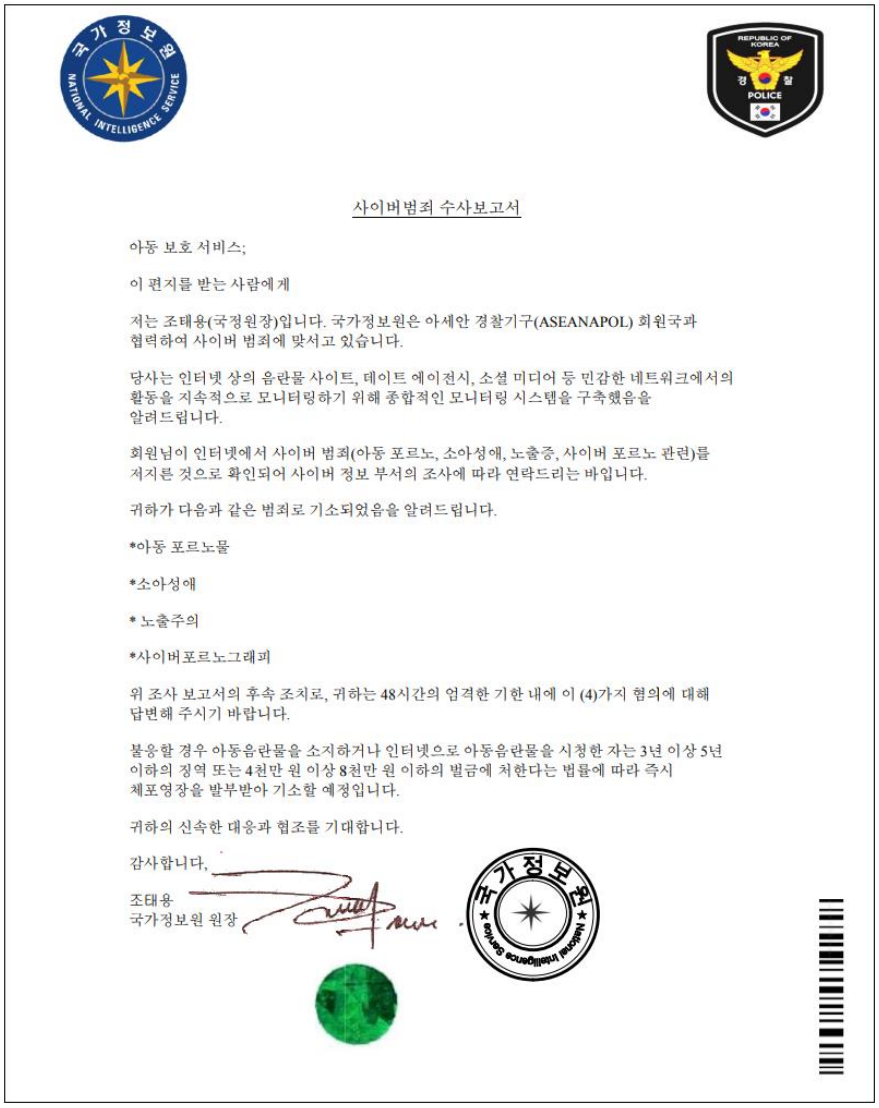
ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.



[그림 2] 국정원 사칭 피싱 메일

해당 피싱 메일에는 첨부된 경찰보고서를 읽어보고 즉시 회신해달라는 내용으로 첨부파일 확인을 유도하며, 첨부된 pdf 파일에는 '사이버범죄 수사보고서' 라는 제목으로 사이버범죄에 기소되어 답변이 필요하며 불응 시 체포될 예정이라는 내용으로 메일 수신자에게 위협을 주고 있습니다.

ESTsecurity Copyright©2024 ESTsecurity Corp. All rights reserved.



사이버범죄 수사보고서

아동 보호 서비스;

이 편지를 받는 사람에게

저는 조태용(국정원장)입니다. 국가정보원은 아세안 경찰기구(ASEANAPOL) 회원국과 협력하여 사이버 범죄에 맞서고 있습니다.

당사는 인터넷 상의 음란물 사이트, 데이트 에이전시, 소셜 미디어 등 민감한 네트워크에서의 활동을 지속적으로 모니터링하기 위해 종합적인 모니터링 시스템을 구축했음을 알려드립니다.

회원님이 인터넷에서 사이버 범죄(아동 포르노, 소아성애, 노출증, 사이버 포르노 관련)를 저지른 것으로 확인되어 사이버 정보 부서의 조사에 따라 연락드리는 바입니다.

귀하가 다음과 같은 범죄로 기소되었음을 알려드립니다.

*아동 포르노물

*소아성애

* 노출주의

*사이버포르노그래피

위 조사 보고서의 후속 조치로, 귀하는 48시간의 엄격한 기한 내에 이 (4)가지 혐의에 대해 답변해 주시기 바랍니다.

불응할 경우 아동음란물을 소지하거나 인터넷으로 아동음란물을 시청한 자는 3년 이상 5년 이하의 징역 또는 4천만 원 이상 8천만 원 이하의 벌금에 처한다는 법률에 따라 즉시 체포영장을 발부받아 기소할 예정입니다.

귀하의 신속한 대응과 협조를 기대합니다.

감사합니다,

조태용
국가정보원 원장

[그림 3] '국가정보원(한국).pdf' 파일

최근 유포된 메일도 최초 발견된 메일과 동일한 내용이며, 첨부파일 해시값 확인 결과 동일한 파일로 확인되었습니다. 또한 첨부파일 분석결과 경찰 보고서를 사칭한 부분 외에 다른 악성행위는 없는 것으로 확인되었습니다.

하지만 지난달 국정원 공지를 통해 피싱 메일임이 밝혀졌음에도 계속 유포되고 있는 상황과 메일 회신을 유도하는 점으로 보아 메일 수신자의 반응을 살펴 이후 공격을 진행하기 위한 사전 작업으로 발송하는 경우일 수 있어 주의가 필요합니다.

또한 ESRC 에서는 해당 첨부파일이 언제든지 악성행위가 추가된 악성파일로 교체되어 유포될 가능성이 있어 지속적인 모니터링을 진행하고 있습니다.

ESTSECURITY Copyright©2024 ESTsecurity Corp. All rights reserved.

㈜이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

www.estsecurity.com