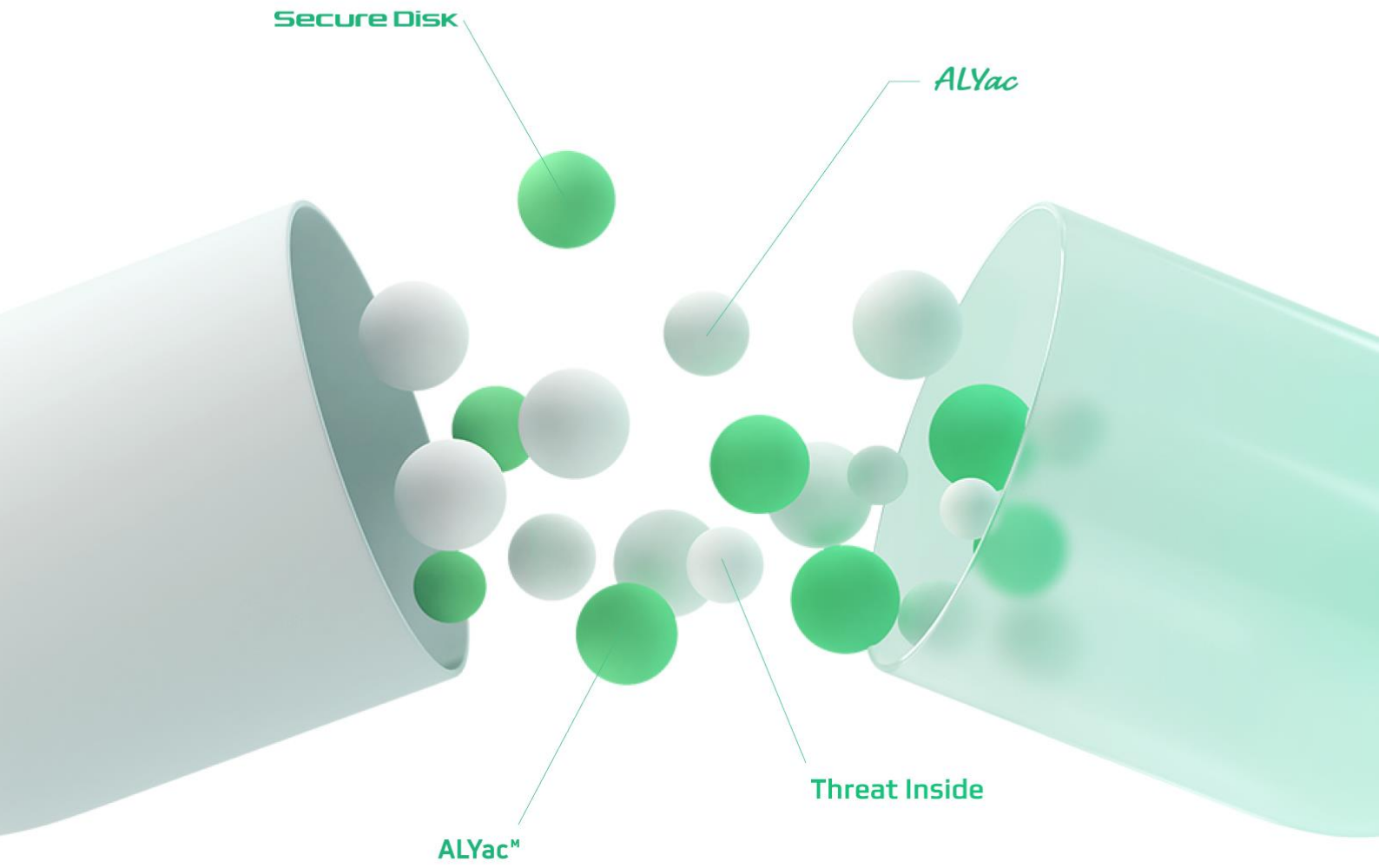
이스트시큐리티
보안동향보고서

No.170
2023/11/24

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



ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

이스트시큐리티 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 08-15

1

악성코드 통계 및 분석

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

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

1. 악성코드 동향

북한 정부의 지원을 받는 해킹조직의 공격이 여전히 강세를 보이고 있습니다.

국가정보원(NCSC)에 따르면 올해 8-9 월 간 북한 해킹조직이 국내 유수의 조선업체를 타깃으로 공격을 시도한 사례를 여러 건 포착하였고, 이들은 내부 직원을 대상으로 피싱 메일을 유포 후 악성코드를 설치하거나 IT 유지보수업체의 PC 를 우회 침투하는 수법 등을 사용하였다고 밝혔습니다. 또한, 북한 해킹조직과 국내 복구대행업체가 사전 모의해 랜섬웨어를 유포하고, 복구업체가 이를 복구할 수 있다 광고해 피해자들로부터 벌어들인 거액의 수익을 나눠 가진 범행도 경찰청 안보수사대를 통해 알려졌습니다.

국내뿐만 아니라 해외에서도 활발한 활동을 이어갔습니다. 소프트웨어 개발 애플리케이션 'TeamCity' 의 서버 원격코드 취약점(CVE-2023-42793)을 악용하고, 디지털 인증서를 사용해 웹 통신을 암호화하도록 설계된 소프트웨어 결함을 악용한 사례, Meta 채용담당자로 위장해 LinkedIn 메시지로 피해자에게 접근한 뒤 프로그래밍 테스트를 가장해 악성코드 유포 및 접근 권한 취득하는 방식 등 북한 정부 지원 사이버 조직의 위협은 나날이 고도화되고 가파른 확장세를 보이고 있습니다.

이스라엘-하마스 전쟁이 심화됨에 따라 반대 진영을 타깃으로 하는 사이버 위협이 고조되고 있습니다.
지난 10 월 7 일 이스라엘과 하마스의 전쟁이 선포된 이후 양국 간의 물리적인 충돌과 더불어 정부 기관 및 언론 기관, 웹 사이트, 애플리케이션 등을 겨냥한 DDos 공격과 Wiper 멀웨어, 피싱 공격 등이 쏟아지고 있습니다. 가짜 트래픽으로 특정 웹사이트와 앱의 과부하 및 접속 장애를 야기하거나 피싱 메일, 정상 애플리케이션 도용 등으로 악성코드를 유포하는 사례가 꾸준히 확인되고 있습니다.

이는 러시아-우크라이나 전쟁 때와 동일한 양상을 보이는 것이며, 이념을 기반으로 한 사이버 범죄 조직들이 전쟁 당사자들과 같은 편에 서서 반대 세력의 기관과 시스템을 공격하는 경우가 보편화되고 있는 흐름입니다. 우리나라도 관련하여 입장을 표명한 뒤 정부 기관, 민간 기업 일부가 이들의 공격 대상으로 지목된 바 있습니다.

폐쇄된 것으로 알려진 QakBot(Qbot) 조직이 여전히 운영 중인 것으로 나타났습니다.

전세계 70 만대 이상의 시스템을 감염시키고 수억 달러의 피해를 입힌 QakBot 은 지난 8 월 FBI 와 미 법무부, 프랑스, 독일 등 국제 사이버 공조(Duck Hunt 작전)를 통해 위협 인프라의 무력화가 발표되었습니다. 하지만, QakBot 배후의 공격자들은 8 월 초부터 여전히 캠페인을 수행하는 것으로 관찰되었습니다. 공격자들은 타깃에게 피싱 이메일을 보내 Knight 랜섬웨어 및 원격 액세스 트로이목마 Remcos, 정보 탈취 악성코드 RedLine 와 DarkGate 백도어를 배포하는 것으로 나타났습니다.

따라서 당시 Dunt Hunt 작전이 QakBot 운영조직의 전체 스팸/피싱 인프라가 아닌 일부 C&C 에만 영향을 미쳤던 것으로 추측되며, 이는 머지 않은 시기에 리빌딩된 QakBot 조직의 광범위한 공격이 재개될 가능성을 시사합니다.

ESTsecurity Copyright©2022 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.

2023 년 10 월에는 Application.Hacktool.BBJ, Trojan.GenericKD.68914091, Trojan.Agent.floxif, Trojan.GenericKD.46017682, Win32.Neshta.A 악성코드가 새롭게 Top 15 에 진입하였습니다.

최상위에 위치한 Application.Hacktool.BBJ 을 포함한 다수의 OS/소프트웨어 불법 인증툴 탐지명(Gen:Variant.Application.Keygen.34, Misc.HackTool.AutoKMS, Misc.HackTool.KMSActivator)이 꾸준히 상위 랭크를 유지하고 있고, 기본적인 Worm/Virus 관련 악성코드(Trojan.Agent.floxif, Trojan.GenericKD.46017682, Trojan.Acad.Bursted.AK, Win32.Neshta.A)도 지속적으로 강세를 보이고 있습니다.

순위	등락	악성코드 진단명	카테고리	합계(감염자 수)
1	New	Application.Hacktool.BBJ	ETC	119,826
2	New	Trojan.GenericKD.68914091	Trojan	96,215
3	↑3	Gen:Variant.Application.Keygen.34	ETC	78,335
4	↓1	Misc.HackTool.AutoKMS	ETC	45,293
5	-	Trojan.DDoS.Nitol.gen	Trojan	42,518
6	↓5	Trojan.GenericKD.38020318	Trojan	28,650
7	New	Trojan.Agent.floxif	Trojan	25,037
8	↑3	Gen:Variant.Jaik.38715	ETC	22,763
9	New	Trojan.GenericKD.46017682	Trojan	20,795
10	↓1	Misc.HackTool.KMSActivator	ETC	20,558
11	↓4	Trojan.Acad.Bursted.AK	Trojan	19,181
12	New	Win32.Neshta.A	Virus	19,144
13	↓11	Gen:Variant.TDss.49	ETC	18,579
14	↓4	Gen:Variant.Sirefef.2727	ETC	17,561
15	-	Exploit.CVE-2010-2568.Gen	Exploit	17,004

*자체 수집, 신고된 사용자의 감염 통계를 합산하여 산출한 순위임

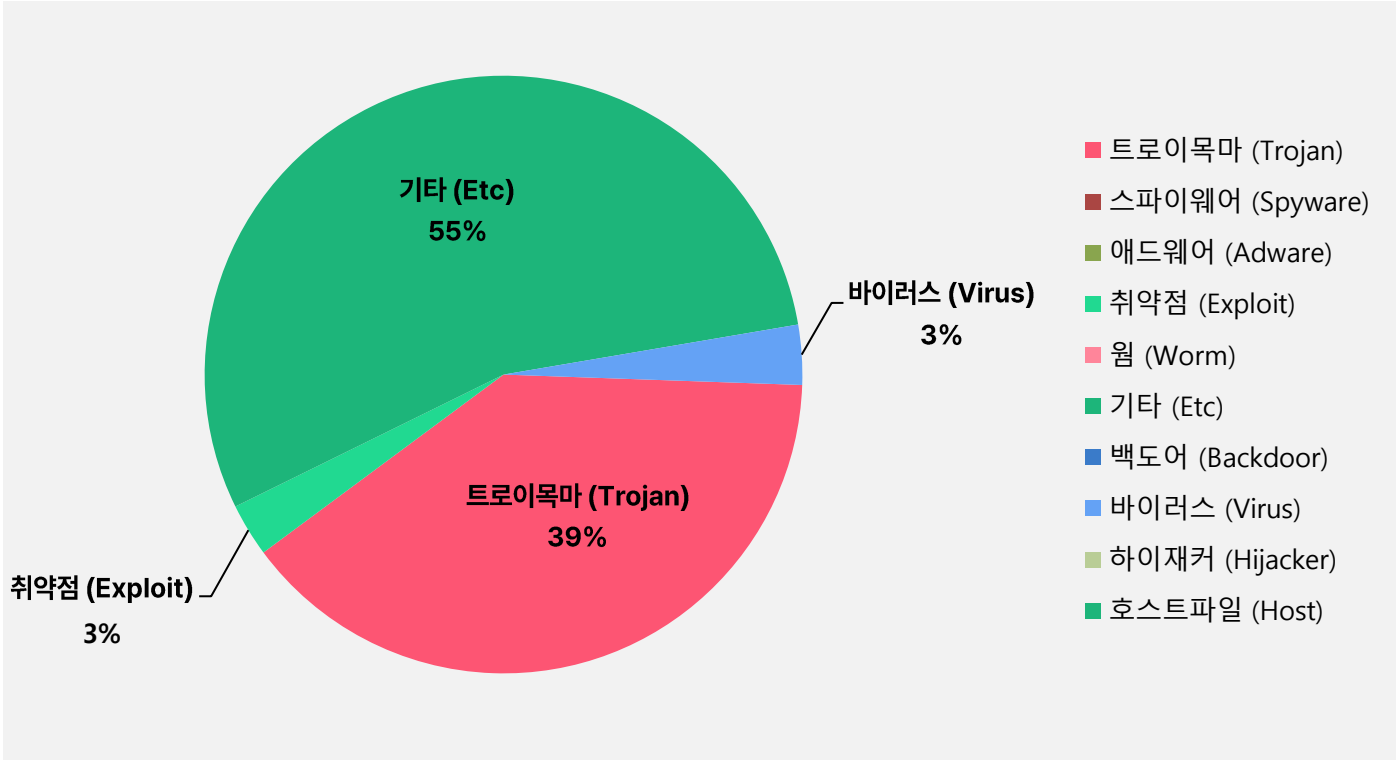
2023 년 10 월 01 일 ~ 2023 년 10 월 31 일

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

악성코드 유형별 비율

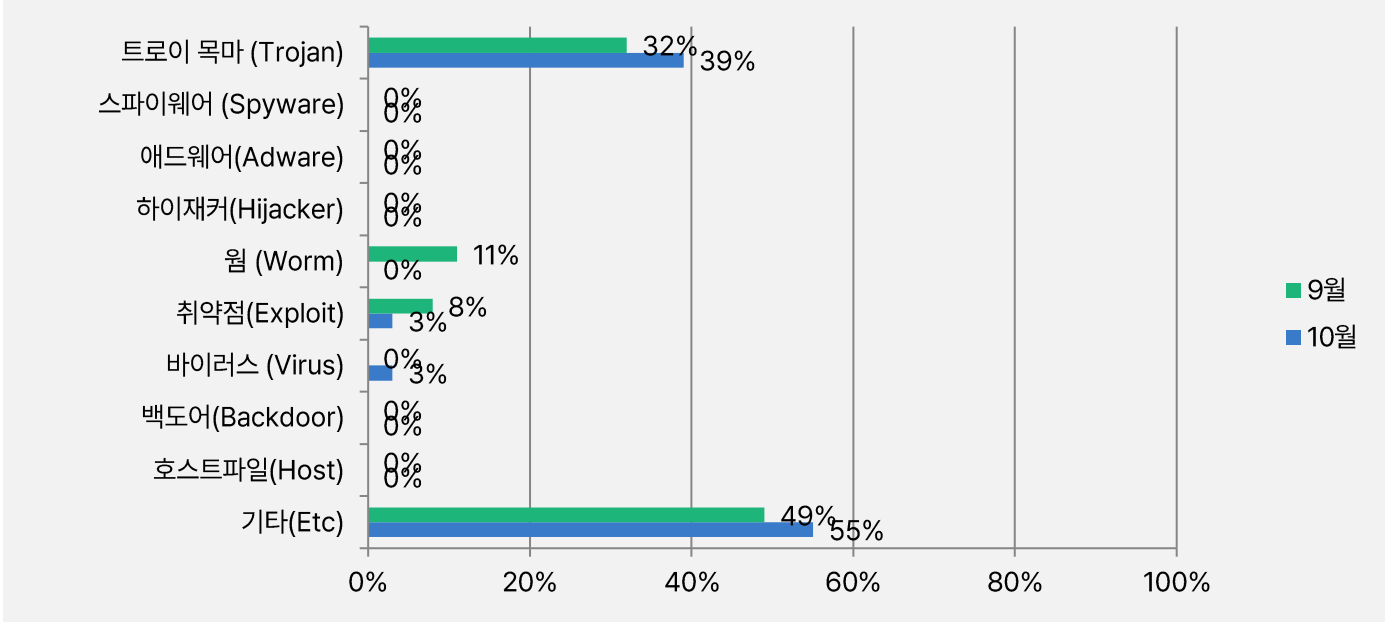
악성코드 유형별 비율에서 기타(ETC) 유형이 55%로 가장 높은 비율로 탐지 되었으며, 그 다음으로 트로이목마(Trojan) 유형이 39%, 바이러스(Virus) 유형이 3%, 취약점(Exploit) 유형이 3%로 확인되었습니다.

2023 년 9 월과 비교하여 전체 감염 건수는 33.7% 증가하였습니다.



카테고리별 악성코드 비율 전월 비교

2023 년 10 월에는 지난 9 월과 비교하여 트로이목마(Trojan) 유형이 7% 증가하였으며, 취약점(Exploit)유형이 5% 감소하였습니다. 기타(ETC)유형은 6% 증가하였고, 바이러스(Virus)유형이 3%로 새로 등장하였습니다.

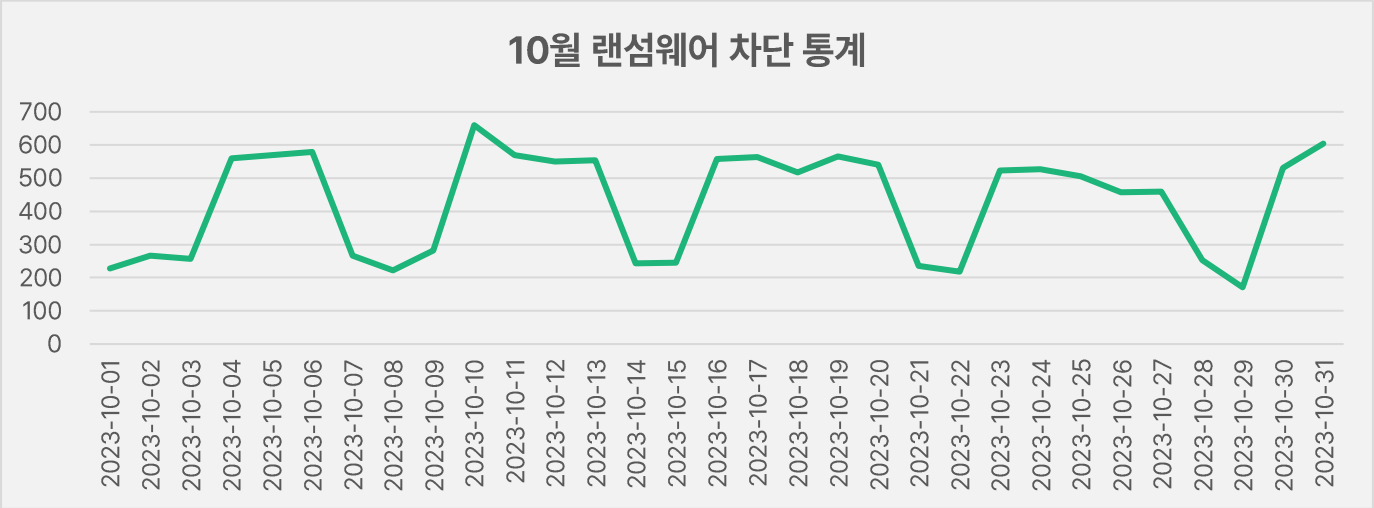


 Copyright©2022 ESTsecurity Corp.All rights reserved.

3. 랜섬웨어 차단 및 악성코드 유포지/경유지 URL 통계

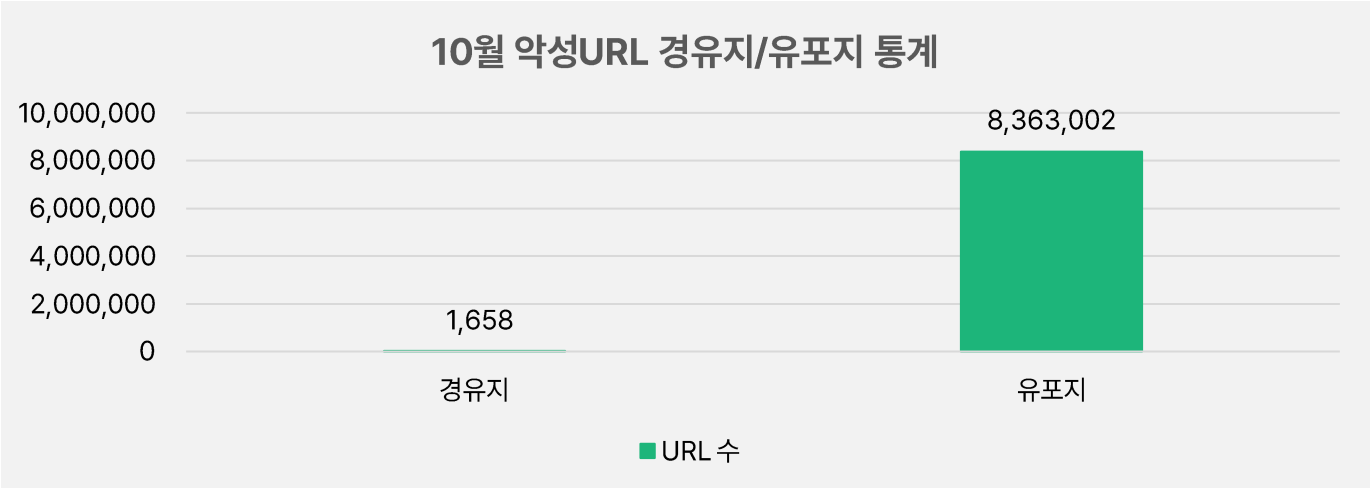
10 월 랜섬웨어 차단 통계

해당 통계는 통합 백신 알약 공개용 버전의 '랜섬웨어 차단' 기능을 통해 수집한 월간 통계로써, DB 에 의한 시그니처 탐지 횟수는 통계에 포함되지 않습니다. 10 월 1 일부터 10 월 31 일까지 총 13,408 건의 랜섬웨어 공격 시도가 차단되었습니다.



악성코드 유포지/경유지 URL 통계

해당 통계는 Threat Inside 에서 수집한 악성코드 유포지/경유지 URL 에 대한 월간 통계로, 10 월 한 달간 총 8,364,660 건의 악성코드 경유지/유포지 URL 이 확인되었습니다. 이 수치는 9 월 한 달간 확인되었던 8,121,108 건의 악성코드 경유지/유포지 URL 수에 비해 약 2.9% 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©2022 ESTsecurity Corp.All rights reserved.

2

최신 보안 동향

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

피싱 페이지를 통해 신용카드 정보 탈취를 시도하는 스미싱 주의!

사용자 카드 정보 유출을 시도하는 스미싱이 발견되어 사용자들의 각별한 주의가 필요합니다.

이번에 발견된 공격은 사용자가 스미싱 내 링크를 클릭하면 최소한의 정보 입력만 유도하고 악성 apk 를 내려주어 설치를 유도하는 일반적인 스미싱과 다르게, 실제 카드 등록 페이지와 유사하게 제작된 피싱 페이지로 접속되어 카드정보 탈취를 시도합니다.

> [BC 카드] 계정을 활성화해야 합니다. 그렇지 않으면 카드가 정지됩니다. hxxps://bc*****[.]com/*/*******

BC 카드 스미싱 메시지

스미싱 내 링크를 클릭하면, 핀번호 설정 페이지를 위장한 피싱 페이지로 접속됩니다.



[그림 1] BC 카드 핀번호 설정 피싱 페이지

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

피싱 페이지에서는 카드번호, 유효기간 및 CVC 번호 뿐만 아니라 주민등록번호, 카드 비밀번호 입력을 요구합니다.

```
function validateCreditCard() {
  // Get the credit card number input element
  const cardNumberInput = document.getElementById('ccnum');

  // Get the card number value
  const cardNumber = cardNumberInput.value;

  // Remove any spaces or dashes from the card number
  const cleanedCardNumber = cardNumber.replace(/[₩s-]/g, '');

  // Check if the card number is valid using the Luhn algorithm
  if (!isValidCardNumber(cleanedCardNumber)) {
    // If the card number is invalid, show an error message and prevent the form from submitting
    alert('정확한 카드번호를 입력해주세요');
    return false;
  }

  // If the card number is valid, allow the form to submit
  return true;
}

function isValidCardNumber(cardNumber) {
  // Use the Luhn algorithm to validate the card number
  let sum = 0;
  let doubleUp = false;
  for (let i = cardNumber.length - 1; i >= 0; i--) {
    let digit = parseInt(cardNumber.charAt(i), 10);
    if (doubleUp) {
      if ((digit *= 2) > 9) digit -= 9;
    }
    sum += digit;
    doubleUp = !doubleUp;
  }
  return sum % 10 == 0;
}
```

[그림 2] 카드번호 검증 코드

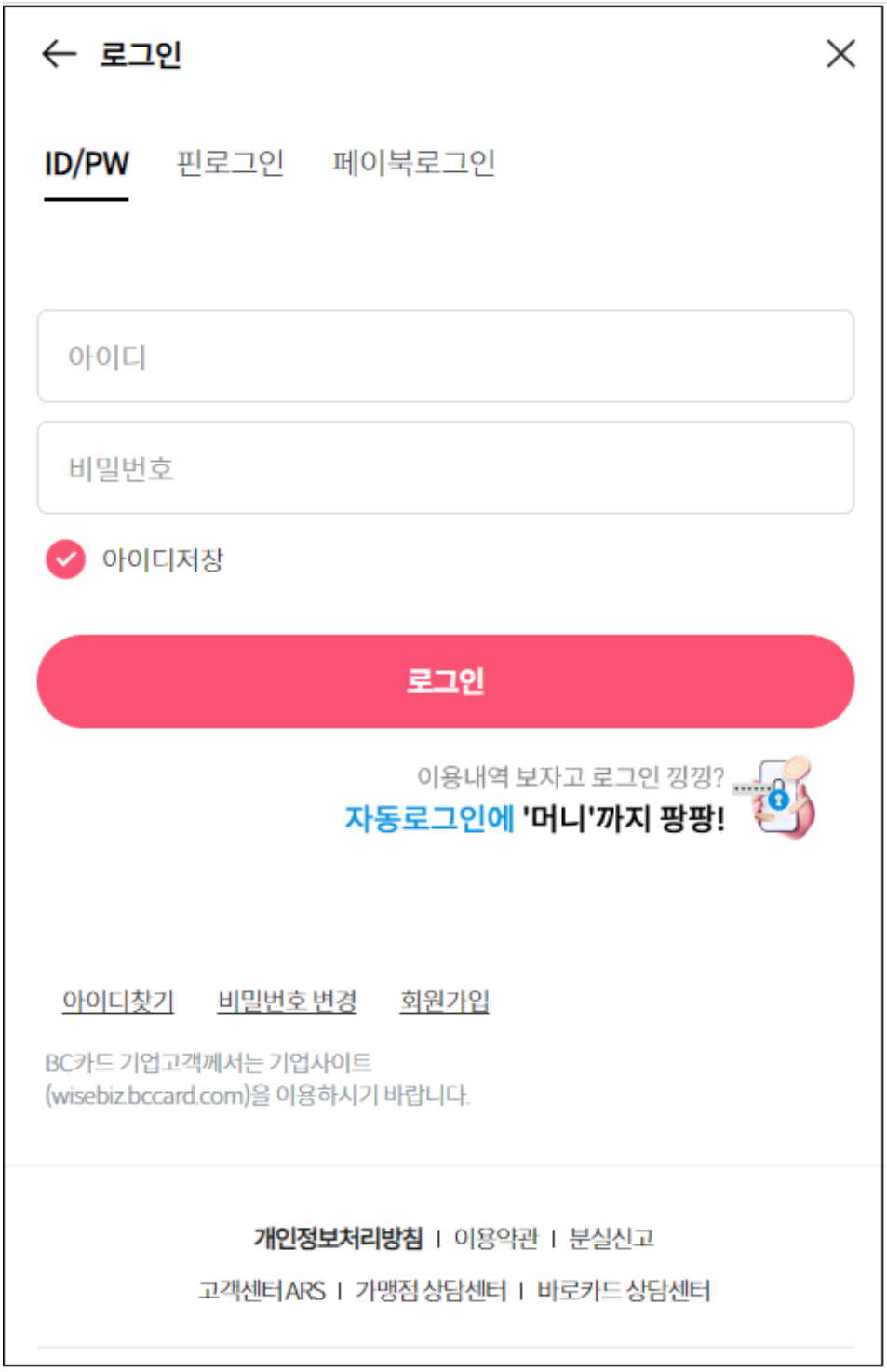
피싱 페이지 내에는 카드번호 검증로직 코드가 포함되어 있어, 임의 카드번호 입력 시 '정확한 카드 번호를 입력해 주세요'라는 팝업이 뜨며 재 입력을 요구합니다.

u1: 홍길동	카드 소유자 이름
cardHolderType: 1	
u2: 83	생년월일
u3: 1	주민번호 뒷자리
ccnum:	카드번호
s4: 10	유효기간 (월)
s5: 2025	유효기간 (년)
s6: 123	CVC 번호
s7: 1234	카드 비밀번호

[그림 3] 공격자에게 전송되는 입력 정보

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

정확한 카드 번호를 입력하면, 입력한 정보는 공격자에게 전송되는 동시에 정상 BC 카드 로그인 페이지로 리디렉션 되며 공격이 종료됩니다.



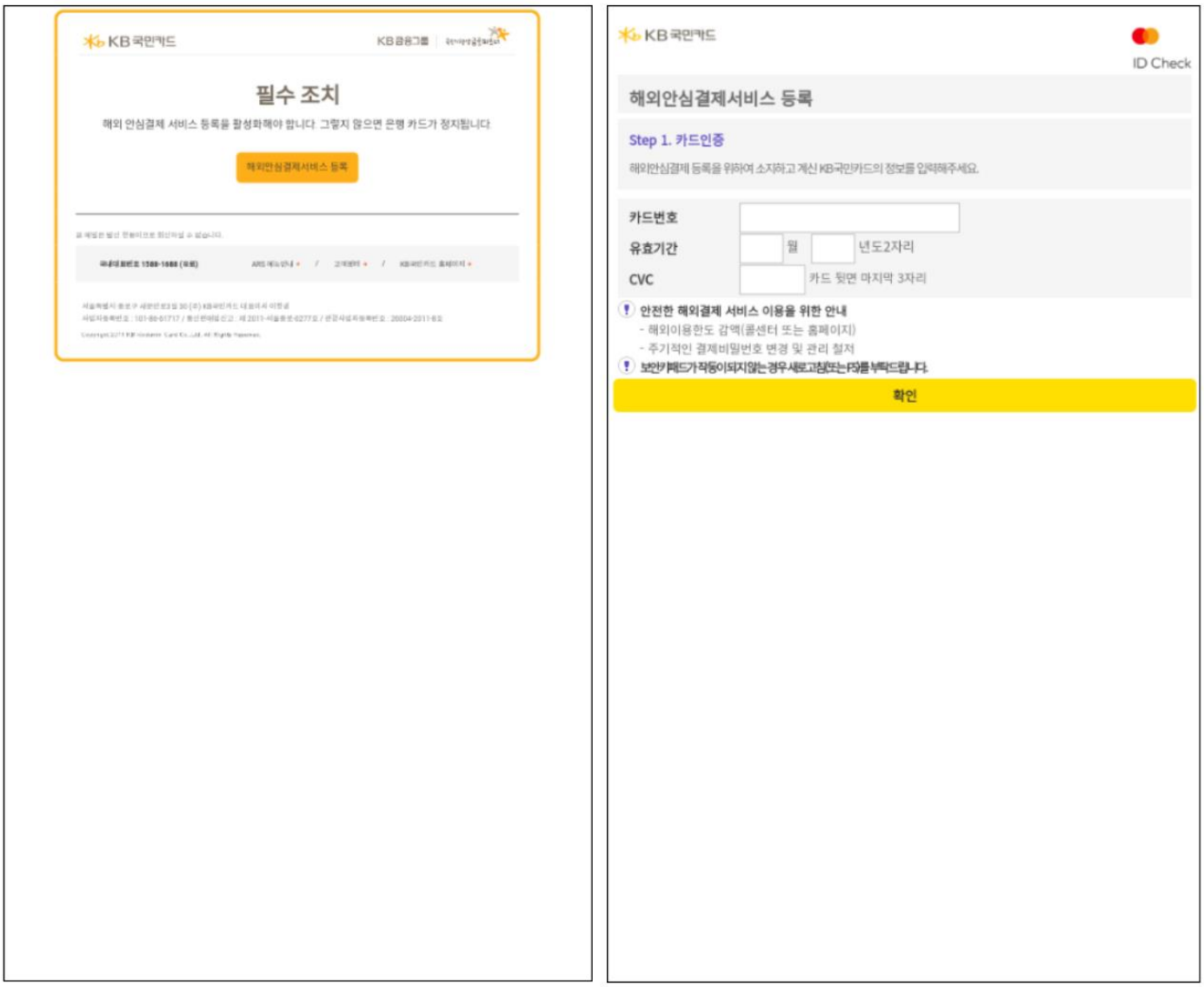
[그림 4] 공격종료 후 리디렉션 되는 정상 페이지

[KB 국민카드] 당신의 은행카드가 정지되었습니다. hxxps://kb*****[.]com/*/*******

KB 국민카드 스미싱 메시지

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

스미싱 내 링크를 클릭하면 피싱 페이지로 접속됩니다.



[그림 5] 링크 클릭 시 접속되는 KB 국민카드 피싱 페이지

피싱페이지에서는 해외 안심결제 서비스 등록 활성화를 하지 않으면 카드가 정지된다는 안내문구와 함께 [해외안심결제서비스 등록] 버튼을 누르도록 유도하며, [해외안심결제서비스 등록] 버튼을 누르면, 해외안심결제 서비스 등록 페이지를 위장한 피싱 페이지로 접속되며 카드번호, 유효기간 및 CVC 번호 입력을 요구합니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

```
<script>
  function validateCreditCard() {
    // Get the credit card number input element
    const cardNumberInput = document.getElementById('strVerificationNum');

    // Get the card number value
    const cardNumber = cardNumberInput.value;

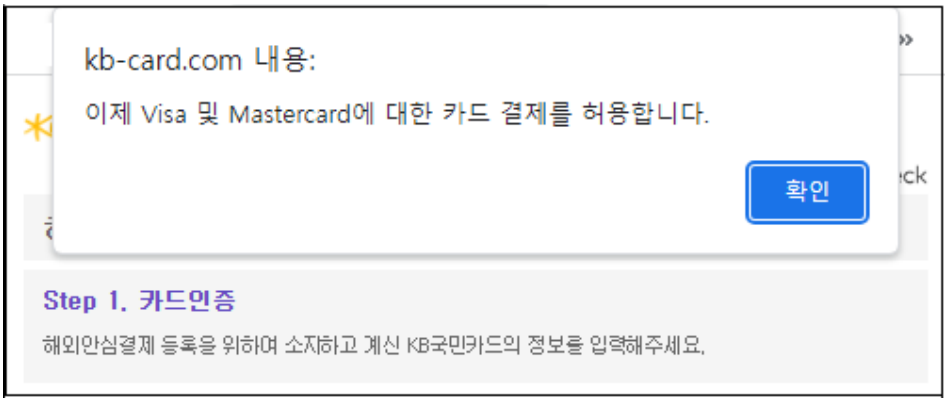
    // Remove any spaces or dashes from the card number
    const cleanedCardNumber = cardNumber.replace(/[\s-]/g, '');

    // Check if the card number is valid using the Luhn algorithm
    if (!isValidCardNumber(cleanedCardNumber)) {
      // If the card number is invalid, show an error message and prevent the form from submitting
      alert('이제 Visa 및 Mastercard에 대한 카드 결제를 허용합니다.');
      return false;
    }

    // If the card number is valid, allow the form to submit
    return true;
  }

  function isValidCardNumber(cardNumber) {
    // Use the Luhn algorithm to validate the card number
    let sum = 0;
    let doubleUp = false;
    for (let i = cardNumber.length - 1; i >= 0; i--) {
      let digit = parseInt(cardNumber.charAt(i), 10);
      if (doubleUp) {
        if ((digit *= 2) > 9) digit -= 9;
      }
      sum += digit;
      doubleUp = !doubleUp;
    }
    return sum % 10 == 0;
  }
</script>
```

[그림 6] KB 국민카드 피싱페이지 내 카드번호 검증 코드



[그림 7] 임의 카드번호 입력 시 뜨는 팝업창

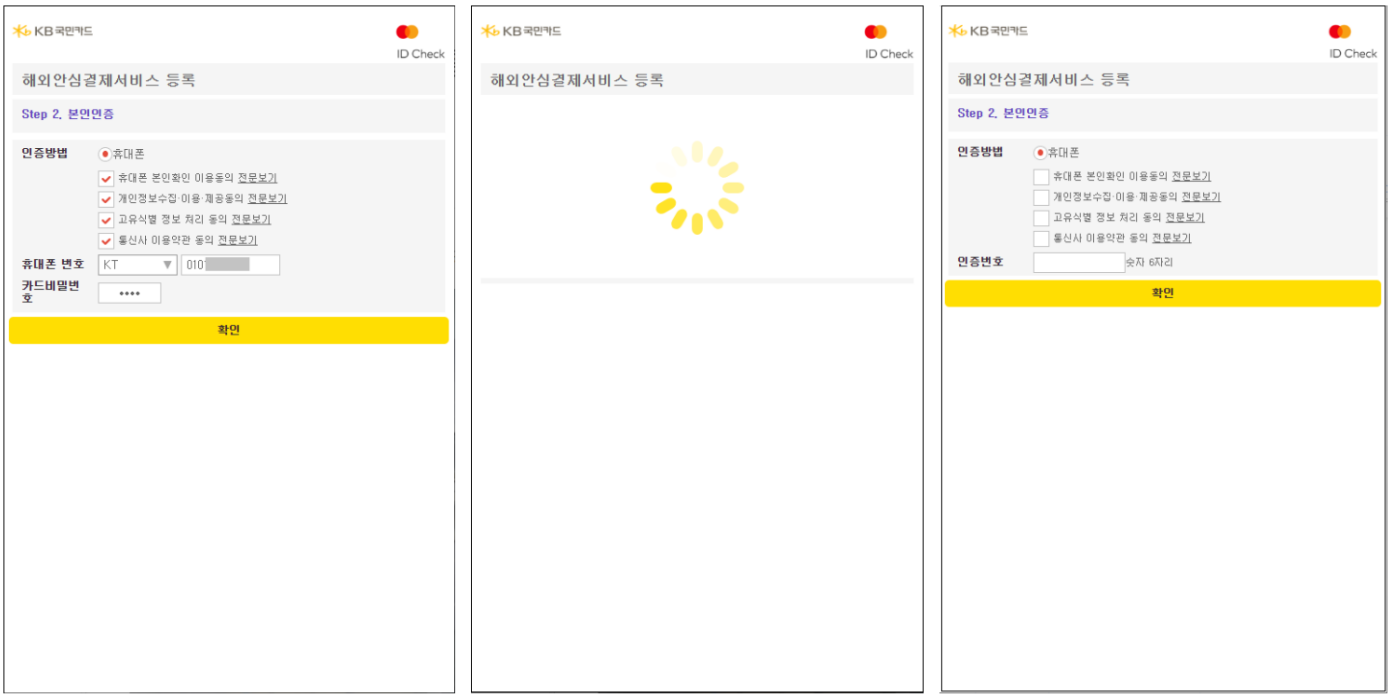
해당 피싱 페이지에도 카드번호 체크 로직이 포함되어 있어, 규칙에 맞지 않는 임의의 카드번호를 넣으면 '이제 Visa 및 Mastercard 에 대한 카드 결제를 허용합니다' 팝업이 뜨며 아무런 동작을 하지 않습니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

e11: 홍길동	카드 소유자 이름
e22: 83	생년월일
e33: 1	주민번호 뒷자리
strVerificationNum11:	카드번호
strExpire2: 11	유효기간 (월)
strExpire1: 26	유효기간 (년)
strVerificationNum: 321	CVC 번호

[그림 8] 공격자에게 전송되는 입력정보

정상 카드번호를 입력하면 입력된 데이터가 공격자에게 전송됨과 동시에 본인인증 피싱 페이지로 이동합니다.



[그림 9] 카드정보 입력 후 접속되는 KB 국민카드 본인인증 피싱 페이지

certType_s: S
agree1: on
agree2: on
agree3: on
agree4: on
telCorp: KT
strPhoneNo1: 010
strPinNo:

[그림 10] 공격자에게 전송되는 추가정보

본인인증 피싱 페이지에서는 통신사와 휴대폰번호, 그리고 또 한번의 카드 비밀번호 입력을 요구하며, 입력한 정보는 추가로 공격자에게 전송되며 공격이 종료됩니다.

 Copyright©2022 ESTsecurity Corp.All rights reserved.

링크 클릭 시 피싱 페이지로 유도하여 신용카드 정보 입력을 유도하는 스미싱 공격방식은 악성앱을 내려주거나, 콜백을 유도하는 최근의 공격 방식과는 다른 새로운 공격방식으로 이러한 공격이 증가할지 지속적인 모니터링이 필요합니다.

카드번호, 유효기간 및 CVC 번호가 유출되면 금전적 손해가 발생할 수 있기 때문에 신용카드 정보와 같은 금융정보 입력 시에는 반드시 주의가 필요합니다.

정상적인 카드 결제 시 주민등록번호 전체 숫자, 카드 비밀번호 네자리를 모두 입력하도록 요구하는 경우는 없다는 점을 반드시 기억하고 있어야 하며, 카드정보 유출이 의심된다면 바로 해당 카드사에 전화하여 카드 사용정지 및 재발급을 받아 유출된 카드의 부정사용을 차단하여 추가 피해를 예방하시기 바랍니다.

ESTsecurity Copyright©2022 ESTsecurity Corp.All rights reserved.

www.estsecurity.com

(주)이스트시큐리티

(우) 06711 서울시 서초구 반포대로 3 이스트빌딩 02.583.4616