월간 악성코드 분석 보고서 (2018-08)

정보 탈취 악성코드 “Orcus RAT”

수산INT 기술 연구소 (CERT)

2018. 08. 23

본 문서는 세계적으로 유명한 ‘Orcus RAT’을 설명합니다. Orcus RAT은 트로잔의 일종으로 사용자 기기에 잠입해 정보를 탈취하는 악성코드입니다.
본 문서는 수산아이앤티 CERT에서 작성되었으며 연구 목적의 활용은 가능하나, 그 외 활용으로 인해 발생하는 문제에 대한 법적 책임은 당사자에 있음을 알려드립니다.

문의처: 기술 연구소 CERT 파트 (SungMin.Rue@soosan.co.kr / KimNamGuy@soosan.co.kr)

SOOSAN INT

목 차

1. 개 요

2018년 상반기 기준으로 은닉사이트에 숨겨진 악성코드 가운데 30%이상이 정보유출과 관련된 것으로 확인되었습니다[1]. 한국인터넷진흥원에 따르면, 정보유출 관련 악성코드 비중은 33.6%로 14.9%인 랜섬웨어 보다 2배 이상 더 많았습니다. 정보유출 관련 악성코드 배포 현황을 세분화해서 살펴보면, 계정 정보유출 (25.3%), 기기 정보유출 (5.8%), 금융 정보유출 (2.1%), 키로깅 (0.4%) 입니다.

이처럼 정보유출 관련 악성 공격이 많은 이유는, 정보가 무형이지만 자산의 가치가 있기 때문입니다. 이에 따라 정보유출 관련 악성코드 툴을 판매하는 사례도 등장하고 있습니다. 대표적인 악성코드 툴로 'Orcus RAT'[2]이 있습니다. 해당 악성코드 툴은 트로잔의 일종으로 일반인도 쉽게 정보유출 악성 공격을 감행할 수 있게 지원합니다.

CERT팀은 Orcus RAT이 '한글파일', '워드파일', '게임' 등 여러 응용 프로그램으로 위장해 정보를 탈취하는 행위를 포착했습니다. Orcus RAT은 감염 기기에서 얻은 정보를 해커에게 보내는 방식으로 정보를 탈취해갑니다. 참고로 Orcus RAT은 일반적인 트로잔처럼 잠입에 쉽게 만들어진 악성코드이기 때문에 개인 기기에 설치한 백신으로 찾아내기가 어렵습니다. 더욱이 Orcus RAT에서 가상환경 탐지 우회, 악성 네트워크 분석 툴 우회하는 기능도 발견되었는데, 이는 보안 전문가가 악성코드를 분석하는 데에 어렵게 합니다.

놀라운 사실은, 위협적인 Orcus RAT을 일반인도 쉽게 사용할 수 있게끔 만들어졌다는 것입니다. 더욱더 놀라운 것은 Orcus RAT이 일반 프로그램으로 분류되고 있는 경우도 많다는 것이다. 구글에서는 Orcus RAT 해커를 위한 모바일 앱도 올라와 있습니다.

Orcus RAT이 정보유출 분야에서 큰 비중을 차지하고 있다는 점을 고려해, CERT팀은 이번 8월호에는 Orcus RAT 분석 내용을 담았습니다.

2장은 Orcus RAT의 개념과 특성을 살펴보고, 이러한 악성 공격이 APT 관점에서 어떤 위험 요소가 되는지를 살펴보겠습니다. 3장에서는 CERT팀에서 분석한 Orcus RAT의 상세 행위정보를 분석한 사례를 소개하면서, 구체적으로 어떻게 정보를 탈취하는지를 설명하겠습니다. 마지막으로 4장에서는 Orcus RAT 대응방안으로 저희 솔루션을 제안합니다.

---

1) 한국인터넷진흥원, "악성코드 은닉사이트 탐지 동향 보고서", 2018년 7월.

2) RAT (Remote Access Trojan): 시스템에 은닉해 원격으로 해커와 통신하는 트로잔의 일종

2. Orcus RAT과 APT 공격

2장에서는 Orcus RAT 개념과 특성을 살펴보도록 하겠습니다. 그리고 APT 공격 관점에서 Orcus RAT 어떤 위협을 가지는지를 살펴보겠습니다.

2.1. Orcus RAT 분석 내용

Orcus RAT 분석 내용을 중심으로 살펴보도록 하겠습니다.

2.1.1. Orcus RAT 등장 배경

[그림 2-1] Orcus RAT 앱 배포 사이트 캡처 화면

Orcus RAT은 2016년에 처음으로 발견된 것으로 알려져 있습니다. 첫 발견 당시 다크웹에서 40달러로 판매되고 있었습니다[3]. 팔로알토는 Orcus RAT의 등장 배경을 추적했는데, 2015년 익명 '소르주스 (Sorzus)'가 해커 포럼에 올린 'Schnorchel' 툴을 기원인 것으로 보고 있습니다. 당시 해당 툴은 오픈소스로 배포되고 있었습니다.

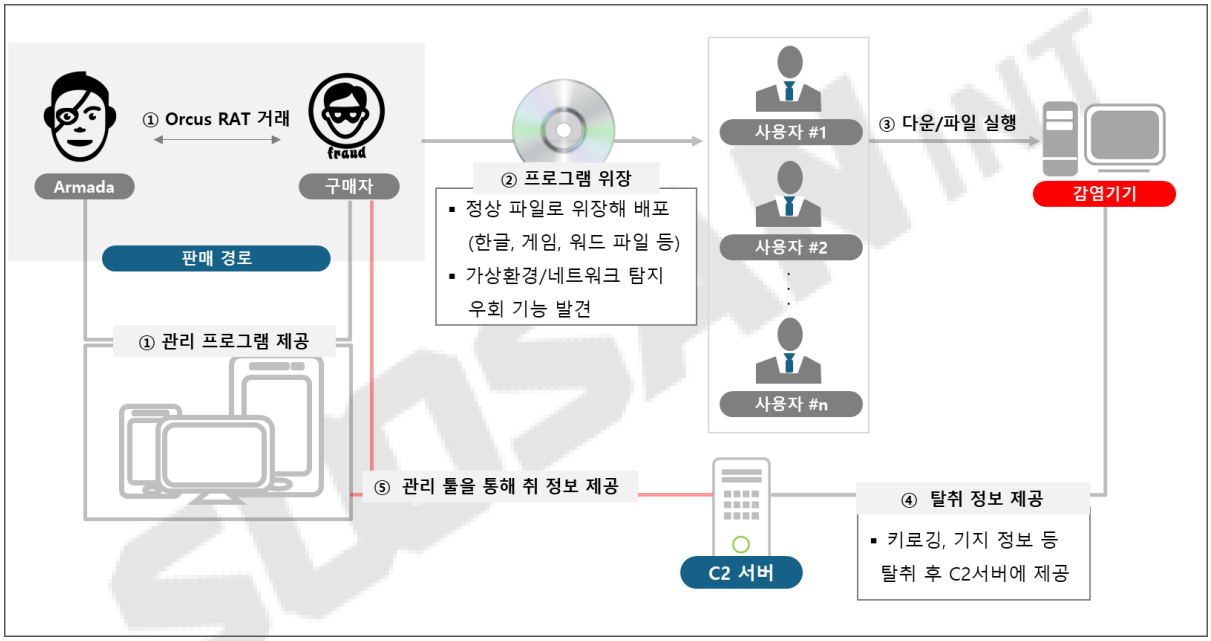
그런데 해커포럼의 익명의 '아르마다 (Armada)'가 소르주스에게 Schnorchel 툴을 유료화 하여 판매할 것을 제안하게 됐고, 이러한 과정에서 Orcus RAT이 등장하게 되었습니다. 소르주스와 아르마다는 비즈니스 파트너 관계를 맺은 것으로 알고 있는데 소르주스는 개발을 담당하고 아르마다는 영업을 담당하고 있는 것으로 알려져 있습니다.

3) Palo Alto (2016), "Birth of an unusual plugin builder.

특이한 사실은, 아르마다가 해당 제품을 영업할 때 Orcus RAT 을 일반 시스템인 것처럼 판매한다는 것입니다.[4] 영업 담당자 아르마다는 전산 담당자를 위한 것으로 불법적인 "Remote Access Trojan"이 아닌 합법적인 "Remote Administration Tool"로 주장하고 있습니다. 이러한 이유로, 다크웹뿐만 아니라 페이스 북 등 SNS 에서도 판매하는 정황이 포착됐습니다. 더욱이 Orcus RAT 사용자 편의를 위해서 이를 지원하는 앱도 다운로드 받을 수 있게 공유하는 사이트도 발견했습니다.

그러나 여러 보안 연구소에서는 Orcus RAT 을 악성코드로 명확히 규정하고 있으며, 저희 CERT 팀 또한 분석해본 결과 Orcus RAT 은 명확한 악성코드로 결론을 내렸습니다.

2.1.2. Orcus RAT 공격 특성



[그림 2-2] Orcus RAT 공격 과정도

그림 2-2는 Orcus RAT의 공격 과정도를 나타낸 것입니다. Orcus RAT의 배포 과정을 조사한 결과, 특정 프로그램으로 위장해 배포되는 경우가 많은 것을 확인했습니다.

Orcus RAT은 트로잔처럼 보안 검열을 피하기 위한 여러 기술이 발견됐습니다. 이는 잠복의 용이성을 향상하는데, 사용자 입장에서 더욱더 위험할 수밖에 없습니다. 대표적인 기능으로 가상화 탐지 우회 기술을 발견했습니다. Orcus RAT은 특정 가상환경에서

4) Krebs on Security, "Canadian Man Behind Popular 'Orcus RAT'"

실행된다는 것을 인지하면 정보탈취와 같은 악성행위를 중지시키는데, 이는 보안 분석을 더욱더 어렵게 합니다. 동적분석 기반 악성 탐지 시스템은 안정성을 위해 별도의 가상환경에 악성코드를 실행해 악성 행위를 탐지하는 경우가 많습니다. 그러므로, Orcus RAT은 가상환경을 인지하고 동작 하지 않는다면 동적분석 기반 악성 탐지 시스템을 우회할 수 있습니다. 네트워크 보안 시스템 우회를 위해 특정 네트워크 분석 툴에서도 동작하지 않는 우회 기술도 발견했습니다.

Orcus RAT이 사용자 시스템에 성공적으로 잠입하면, 감염기기의 다양한 정보를 C2 서버로 전송하게 됩니다. 정보 탈취 유형은 감염자에게 위협적으로 많다. 키로거, 화면 정보, 웹캠, 마이크로폰, 자동 원격 관제, 패스워드 등을 탈취할 수 있도록 고안돼 있습니다.

한 가지 재미있는 사실은, 해커를 위한 관리자 프로그램을 제공한다는 것입니다. 따라서 해커는 쉽게 탈취 정보 현황을 볼 수 있습니다.

2.2. APT 공격 관점의 Orcus RAT

Orcus RAT은 중요 정보를 탈취한다는 점에서 위협적인 악성코드로 평가할 수 있습니다. 더욱이 고도의 우회 수법 기술이 적용됐다는 점과 사용자가 이를 인지하기 쉽지 않다는 점은 고려했을 때, Orcus RAT은 매우 위협적인 악성코드로 평가할 수 있습니다.

특히 APT (Advanced Persistent Threat)에서 보았을 때 Orcus RAT은 매우 효과적인 공격 수단으로 평가할 수 있습니다. APT는 특정 목표물을 대상으로 지속적인 공격을 가하는 사이버 공격 수법을 뜻합니다. APT 공격은 크게 시스템 침투, 잠입, 그리고 목표물 공격으로 나눌 수 있습니다.

이 때 Orcus RAT은 목표물 공격으로 이어지게 끔 하는 데에 매우 유용한 수단이 될 수 있습니다. Orcus RAT은 여러 우회 기술을 가지고 있기 때문에 시스템 침투 시에 쉬울 수 있습니다.

아울러 잠입단계에서도 유용합니다. 대부분 APT 공격은 한 번에 목표물 공격에 성공하지 않습니다. 여러 과정을 거치면서 목표물 접근에 대한 정보를 획득하여 공격에 성공하는 경우가 많은데, 이때 과정이 잠입에 해당합니다. Orcus RAT은 정보 탈취형과 은닉형에 고안된 악성코드입니다. 이러한 특성은 목표물 대상 접근에 매우 유용하게 합니다.

정리하면, Orcus RAT은 매우 위협적인 악성코드로 평가할 수 있습니다. 자체적인 위험성도 내포하고 있지만, APT 공격에도 유용하게 활용될 수 있기 때문입니다.

3. 상세 행위 분석 (Orcus RAT)

수산INT CERT에서는 Orcus RAT을 실제로 분석해 보았습니다. 분석 내용은 다음과 같습니다.

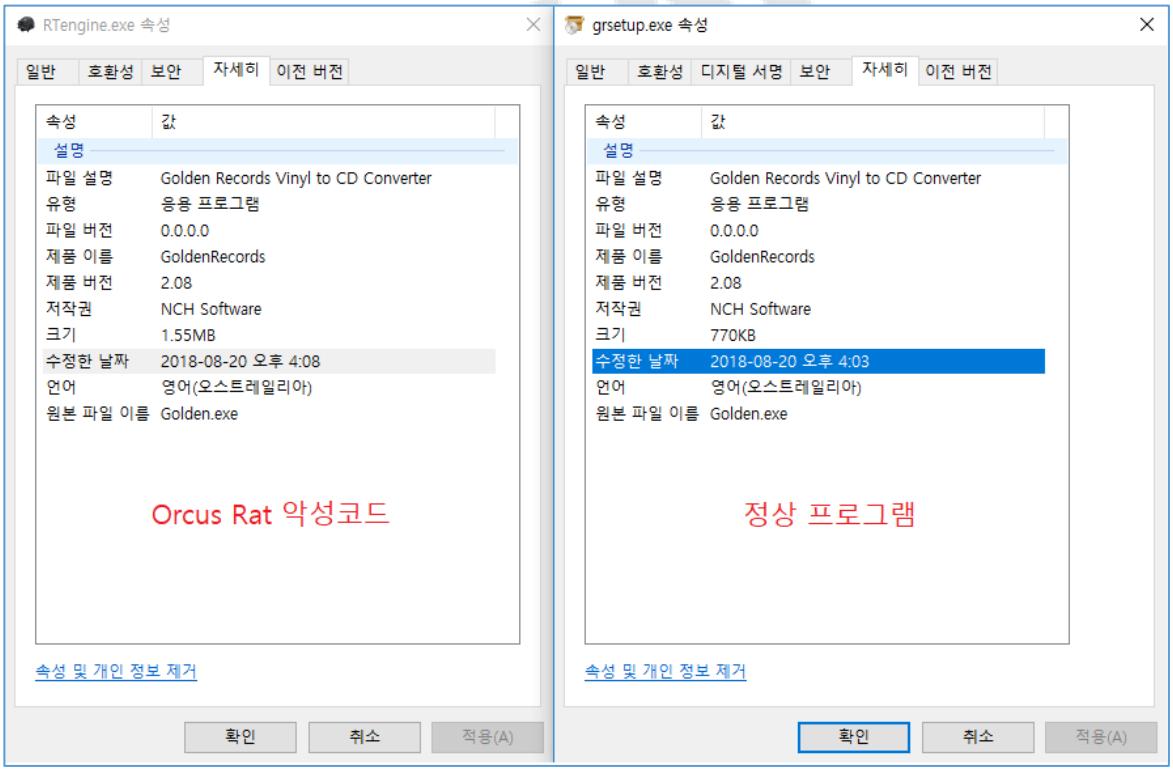
3.1 분석 파일 정보

분석 파일명은 "**[임의로 지정 된 파일명].exe**" 입니다.

해당 파일 해시 정보는 아래와 같습니다.

- MD5: 8559ea29b2819d2580dd0ab237005373
- SHA-1: 5b17c72761ee8a905f4c6956c8ce82db2d2d54f4
- SHA-256: 2133dfa771bfcd154a677b6cafcad20eb703afbd2fe91a305d165bd14504da25

해당 악성 파일은 밑의 그림에 보이는 것 과 같이 정상 프로그램 **(Golden Recods Vinyl to CD Converter)** 으로 위장하기 위하여 파일 설명을 똑같이 하였습니다.

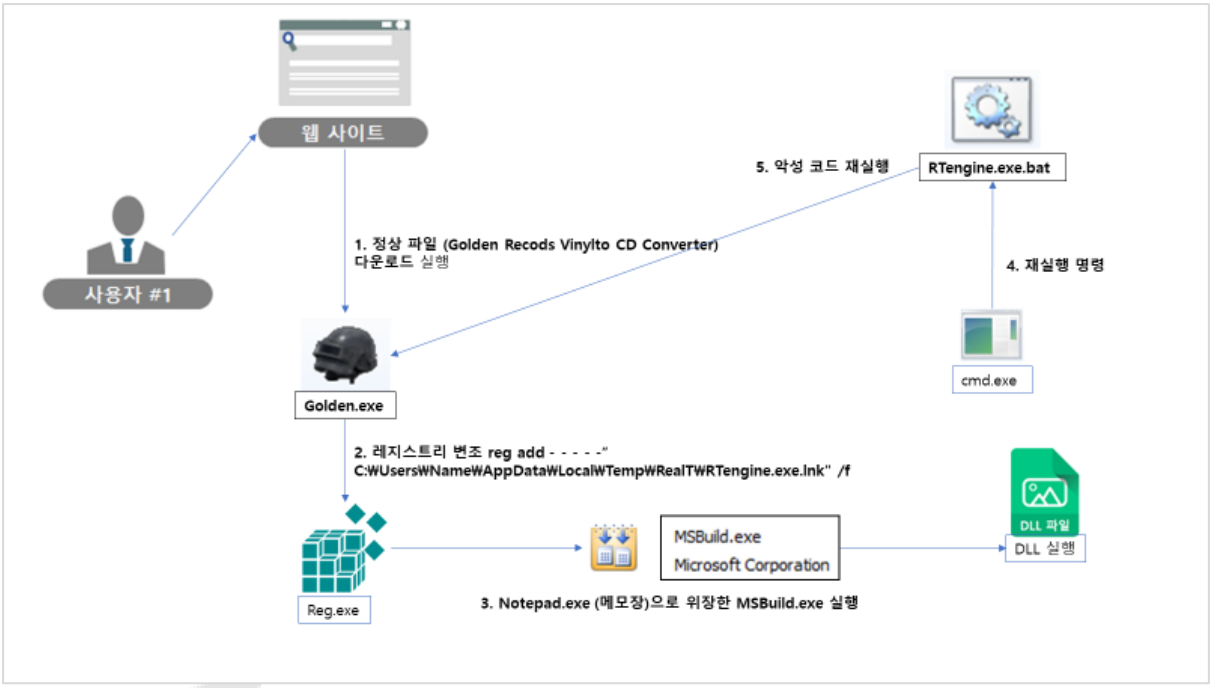


[그림 3-1] 악성 파일 과 정상 파일 설명

3.2 실행 증상

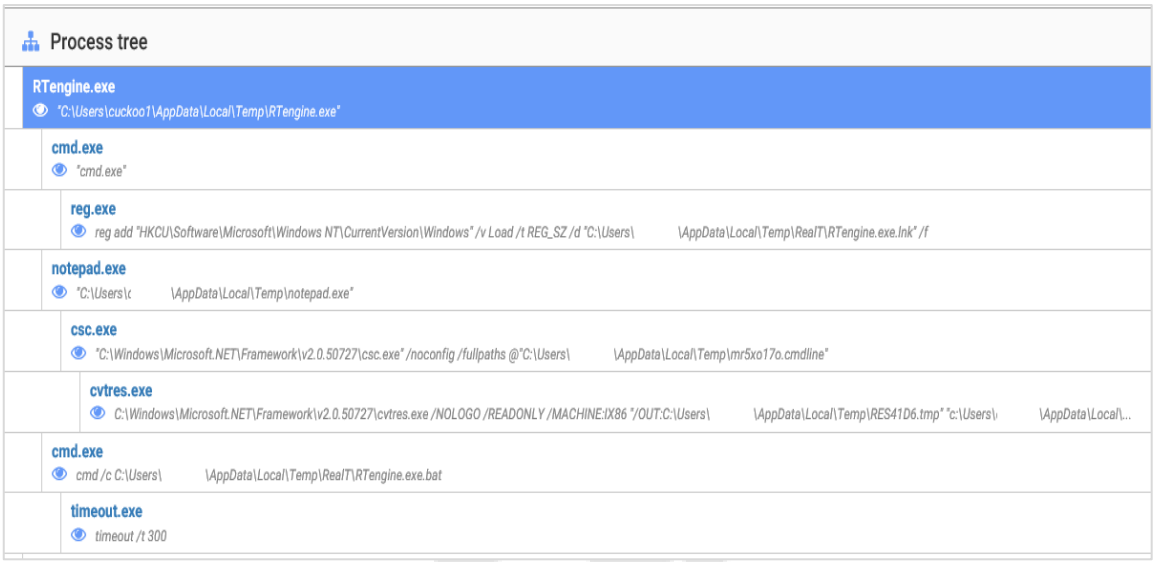
Orcus RAT 을 분석한 결과 아래와 같은 프로세스로 동작을 하였습니다 (그림 3-2 참조).

1. 정상 파일 (Golden Recods Vinylto CD Converter) 다운로드 및 실행
2. 레지스트리 변조 reg add를 사용하여 레지스트리 추가 "Golden.exe"를 복제하여 다른 폴더에 옮긴 것을 실행하는 명령어
3. Notepad.exe (메모장)로 위장한 MSBuild.exe를 이용하여 스크립트 빌드 후 악성 DLL 실행
4. Cmd 명령어를 통하여 Notpad.exe 실행 확인 후 없을 경우, 악성파일 재실행



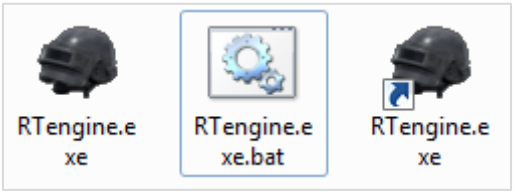
[그림 3-2] Orcus RAT 실행 과정

[그림 3-3]에서의 "RTengine.exe" 악성 파일은 [그림 3-1] 그림과 같이 정상적인 프로그램으로 위장하여 사용자들을 속이기 위한 악성 파일이며, 파일 아이콘은 온라인 게임에 나오는 아이템을 아이콘으로 본 뜬 것으로 보안 특정 대상으로 한 공격이 아닌 불특정 다수에게 유포하기 위해서 사용자들에게 익숙한 아이콘을 만든 것으로 보여집니다. 밑의 그림은 자동 분석 시스템을 통하여, 도출된 프로세스 구조입니다.



[그림 3-3] Process Tree

위의 그림에 "RTengine.exe" 악성 파일 실행 후 "reg.exe" (레지스트리 관련 파일)로 변조를 하는 흔적이 보여집니다. 변조 내용은 "C:₩Users₩????₩AppData₩Local₩Temp₩RealT" 폴더에 자기자신을 복제 및 bat 파일을 생성 하게 됩니다.

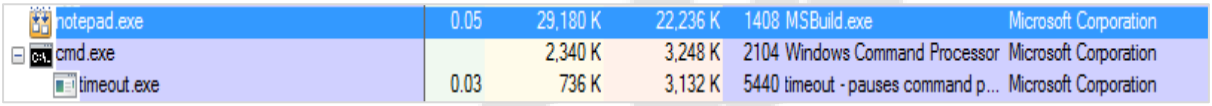


[그림 3-4] 악성파일 자기자신 복제

[그림 3-5]는 "C:₩Users₩????₩AppData₩Local₩Temp₩RealT" 폴더에 설치 되어있는 RTengine.exe.bat 스크립트 내용이며, 300초의 간격을 두어 "RTengine.exe"에서 생성한 또 다른 파일인 "notepad.exe" (notepad로 위장한 MSBuild.exe 파일) 프로세스가 있는지 확인하고 없다면 "RTengine.exe" 악성 파일을 재실행 하게 됩니다. 이러한 점을 보아 생성 한 "notepad.exe" 파일은 악성 행위에 중요한 역할을 하는 것으로 추측이 가능합니다.

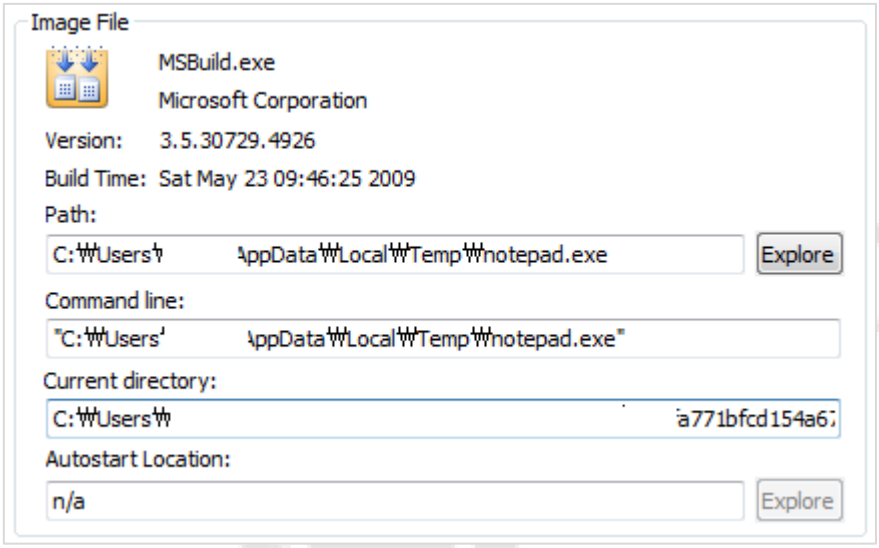
```
:_Start
timeout /t 300
tasklist /nh /fi "imagename eq notepad.exe" | find /i "notepad.exe" >nul && (
Goto _Start
) || (
 Start /W "" "C:\Users\test\AppData\Local\Temp\RealT\RTengine.exe"
Goto _Start
)
```

[그림 3-5] RTengine.exe.bat 파일 명령어



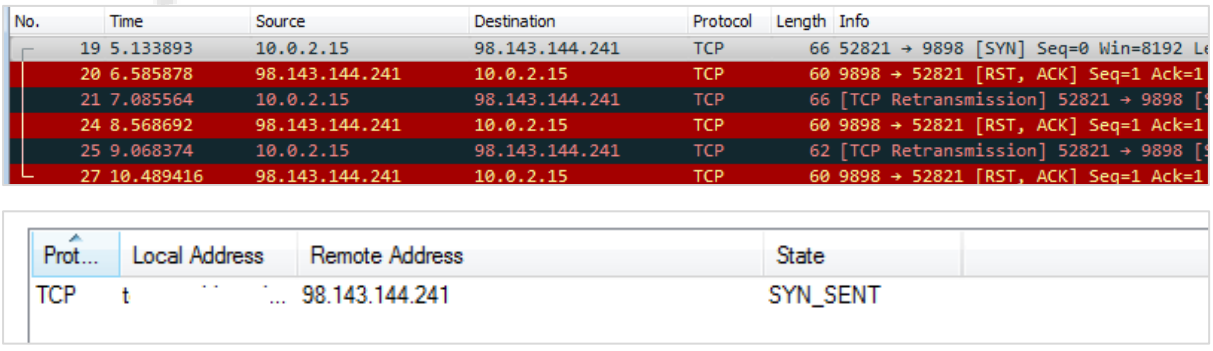
[그림 3-6] 프로세스 Notepad.exe(MSBuild.exe) 실행

[그림 3-7]은 "notepad.exe"의 속성 사진 이며, "MSBuild.exe"를 이름만 "notepad.exe"로 바꾼 것을 확인 할 수 있습니다. 그리고 "MSBuild.exe" 파일의 역할은 Visual Studio에서 사용하는 빌드 역할을 하며, Visual Studio와 차이점은 솔루션이나 프로젝트 등 스크립트만 있어도 MSBuild.exe를 사용하여 현재 환경에 맞추어 빌드하여 줍니다. 이 점을 이용하여 악성 스크립트 생성 및 실행을 하고, 이러 한 과정에서 TCP (C&C) 통신 흔적을 발견 하였습니다.



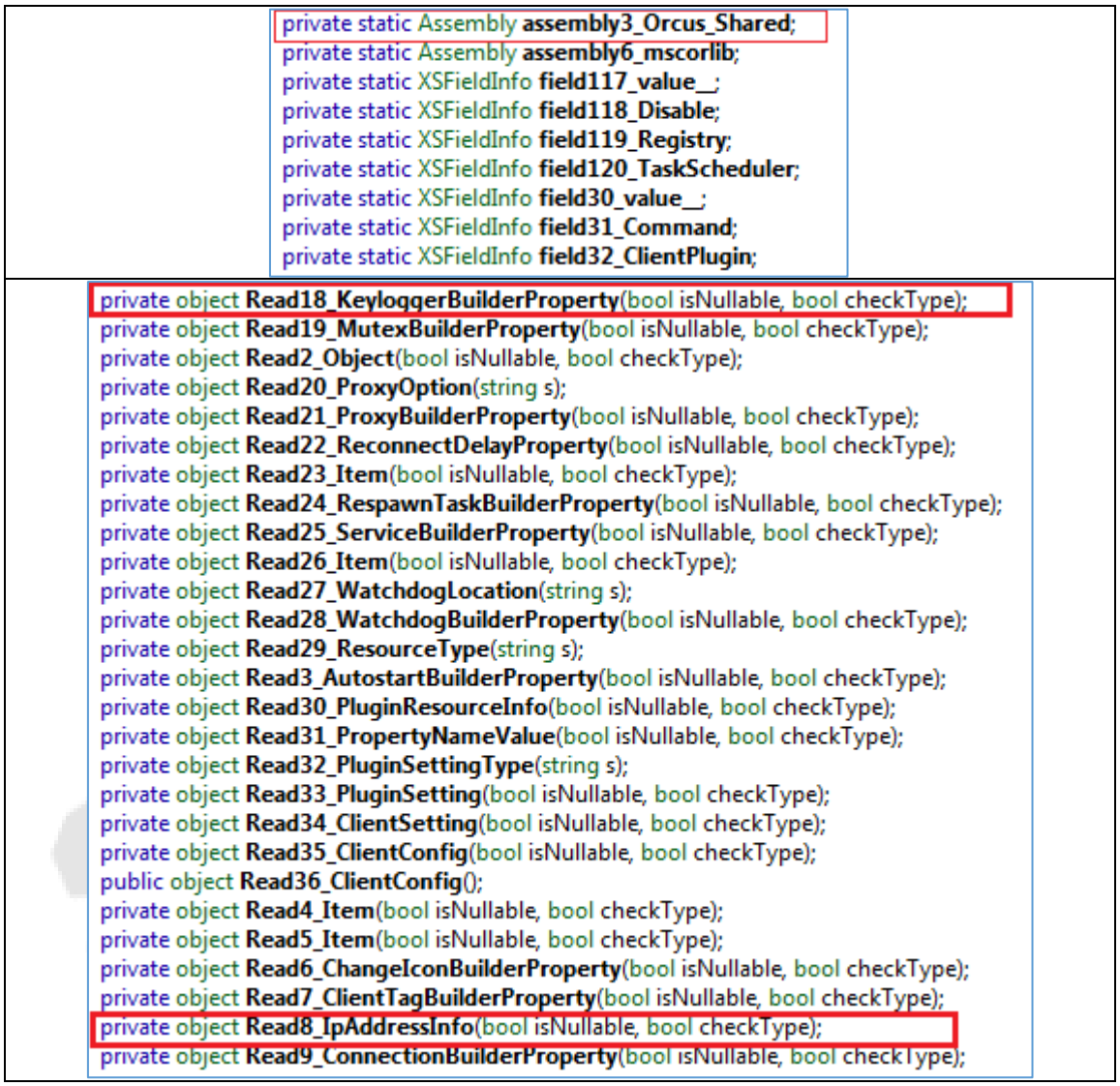
[그림 3-7] MSBuild.exe

[그림 3-8]은 현재 통신은 되지 않지만 분석 컴퓨터 IP(10.0.2.15)에서 특정IP (98.143.144.241) C&C로 시도한 흔적을 발견하였습니다.



[그림 3-8] 네트워크 통신 흔적

"MSBuild.exe"에 의해서 스크립트 빌드가 되어진 DLL 파일 내용 중 일부분을 발췌하였습니다. 이러한 과정에서 Orcus라는 원격제어 소프트웨어의 특정 문자열을 찾을 수 있었으며, 해당 문자열 뿐만 아니라 Keylogger , IpAddressInfo 등 의심되는 함수 명들을 찾을 수 있었습니다.



[그림 3-9] Orcus Software 흔적

이러한 소스코드의 행위들은 IP 정보, 사용자 키 후킹 등 정보유출이 가능한 행위들로 원격제어 접속을 하려는 목적이 보여지는 악성코드 입니다.

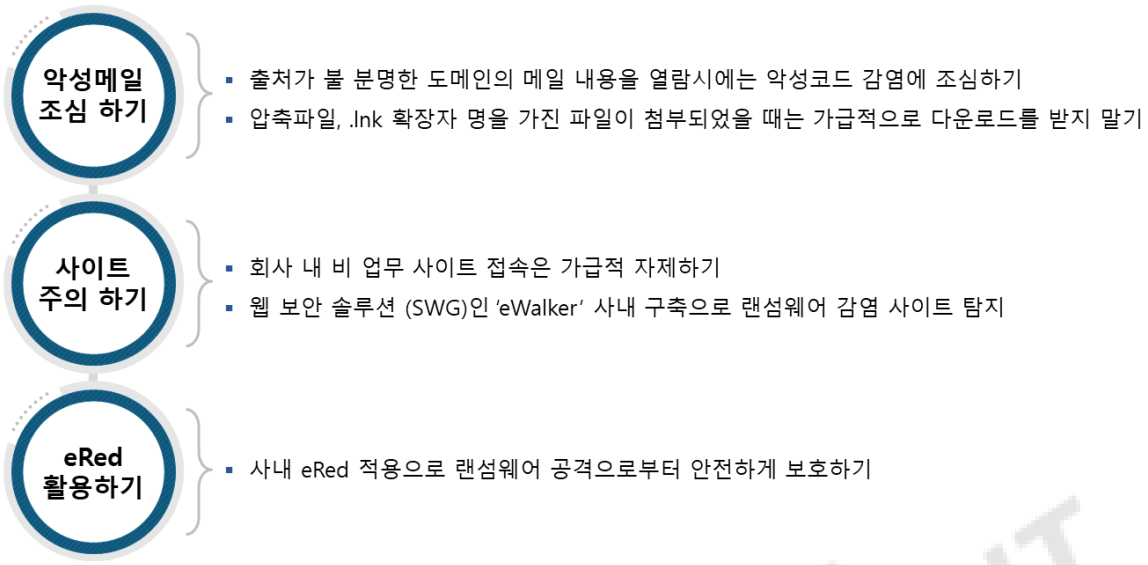
[표 3-1] 악성 파일 C&C IP

C&C (IP)	98.143.144.241

```
int readerCount = base.ReaderCount;
while ((base.Reader.NodeType != XmlNodeType.EndElement) && (base.Reader.NodeType != XmlNodeType.None))
{
   if (base.Reader.NodeType == XmlNodeType.Element)
   {
      if ((!flagArray[0] && (base.Reader.LocalName == this.id50_Ip)) && (base.Reader.NamespaceURI == this.id2_Item))
      {
         prop44_Ip[o] = base.Reader.ReadElementString();
         flagArray[0] = true;
      }
      else if ((!flagArray[1] && (base.Reader.LocalName == this.id51_Port)) && (base.Reader.NamespaceURI == this.id2_Item))
      {
         prop45_Port[o] = XmlConvert.ToInt32(base.Reader.ReadElementString());
         flagArray[1] = true;
      }
      else
      {
         base.UnknownNode(o, ":Ip, :Port");
      }
   }
   else
   {
      base.UnknownNode(o, ":Ip, :Port");
   }
```

[그림 3-10] IP Address Info 함수

4. 대응방안



[그림 4-1] 갠드크랩 2.1 대응 방안

1. **악성메일 조심하기**

   출처가 불 분명한 메일은 가급적 열람하지 않는 것이 좋습니다. 그리고 압축파일 혹은 확장자가 .lnk인 경우에는 악성 파일로 의심해볼 필요가 있습니다.

2. **사이트 방문 주의 하기**

   웹 사이트 경로로 사용자를 감염 시키기도 합니다. 따라서 의심스러운 사이트 방문에 주의할 필요가 있습니다. 그러나 일반 사용자가 이를 판별하기란 쉽지 않습니다. 이러한 한계점을 eWalker 제품 구매로 극복할 수 있습니다. eWalker는 매일 **3만 개가 넘는 악성 사이트를 신규로 업데이트 하고 있어서**, 사용자가 악성 사이트에 접속하는 것을 원천적으로 차단합니다. 따라서 **eWalker 제품으로 Orucus RAT 감염을 예방할 수 있습니다.**.

3. **eRed 활용하기**

   eRed는 화이트 리스트 기반으로 허용되지 않은 프로세스 실행을 원천적으로 차단하는 보안 기술입니다. 그러므로 eRed는 랜섬웨어와 같은 악성 공격 프로세스를 원천적으로 차단합니다. 더욱이 eRed의 동작은 게스트 OS 하부의 하이퍼바이저 OS에 동작하기 때문에 차단 행위를 노리는 악성 공격에도 대응이 가능합니다. **실제로 Orcus RAT을 eRed에 적용해 보았는데, 악성행위를 원천적으로 차단하는 것을 확인했습니다**.

2018 년 수산 INT 보안 연구 보고서 발간 내역

월간 악성코드 분석 보고서

2018-01 호: 가상화폐 채굴 악성코드 분석 (2018 년 01 월)
2018-02 호: UBoat Rat 분석 보고서 (2018 년 02 월)
2018-03 호: 평창올림픽 파괴 악성코드 분석 보고서 (2018 년 03 월)
2018-04 호: 웹으로 감염시키는 악성코드 '헤르메스' 분석 (2018 년 04 월)
2018-05 호: 국내 맞춤형 랜섬웨어 '갠드크랩' (2018 년 05 월)
2018-06 호: 서비스형 랜섬웨어 표본 '갠드크랩 3.0' (2018 년 06 월)
2018-07 호: 키보드 정보로 중요 정보 유출 시키는 '키로거' (2018 년 07 월')
2018-08 호: 정보 탈취 악성코드 "Orcus RAT" (2018 년 08 월)

감사합니다.

글로벌 네트워크 보안 솔루션 전문기업

SOOSAN INT

서울특별시 강남구 밤고개로1길 10, 3층(수서동, 현대벤처빌)

Tel 02.541.0073 | **Fax** 02.541.0204

E-mail QI@soosan.co.kr

HP http://www.soosanint.com