Operação PANDA-19: hackers chineses impulsionam a cadeia de infecção cibernética COVID-19

Introdução

A Check Point Research descobriu uma nova campanha contra o setor público da Mongólia, aproveitando o temor sobre o Coronavírus para disseminar uma implementação de malware anteriormente desconhecido ao alvo.

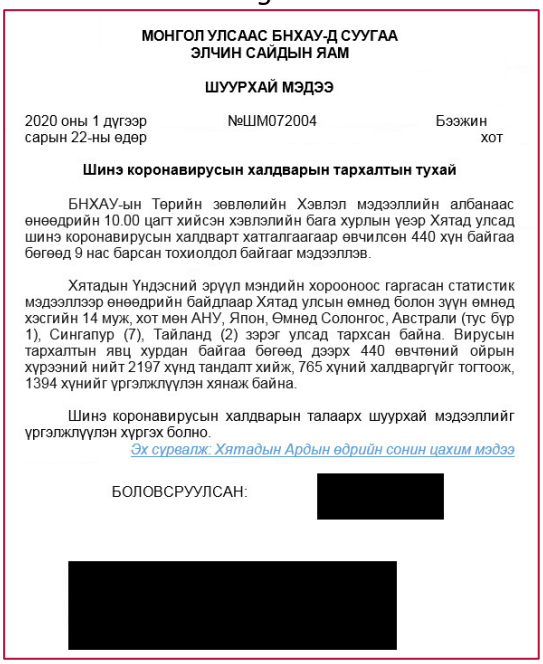
Uma análise mais detalhada dessa campanha permitiu aos pesquisadores da Check Point vinculá-la a outras operações, realizadas pelo mesmo grupo sem nome, que datam de 2016. Ao longo dos anos, essas operações tiveram como alvo diferentes setores em vários países, como a Ucrânia, Rússia e Bielorrússia.

Este relatório é uma análise completa dos TTPs utilizados ao longo dessa campanha, da infraestrutura e das novas ferramentas descobertas durante a pesquisa da equipe da Check Point sobre o que acreditam ser um agente de ameaças ou atacante baseado na China.

Documentos suspeitos

A investigação começou quando os pesquisadores identificaram dois documentos suspeitos de RTF enviados a uma entidade do setor público da Mongólia. Os documentos encontrados estão no idioma mongol, com um deles supostamente escrito pelo Ministro das Relações Exteriores da Mongólia:

Original



МОНГОЛ УЛСААС БНХАУ-Д СУУГАА
ЭЛЧИН САЙДЫН ЯАМ

ШУУРХАЙ МЭДЭЭ

2020 оны 1 дүгээр сарын 22-ны өдөр | №ШМ072004 | Бээжин хот

Шинэ коронавирусын халдварын тархалтын тухай

БНХАУ-ын Төрийн зөвлөлийн Хэвлэл мэдээллийн албанаас өнөөдрийн 10.00 цагт хийсэн хэвлэлийн бага хурлын үеэр Хятад улсад шинэ коронавирусын халдварт хатгалгаагаар өвчилсөн 440 хүн байгаа бөгөөд 9 нас барсан тохиолдол байгааг мэдээллэв.

Хятадын Үндэсний эрүүл мэндийн хорооноос гаргасан статистик мэдээллээр өнөөдрийн байдлаар Хятад улсын өмнөд болон зүүн өмнөд хэсгийн 14 муж, хот мөн АНУ, Япон, Өмнөд Солонгос, Австрали (тус бүр 1), Сингапур (7), Тайланд (2) зэрэг улсад тархсан байна. Вирусын тархалтын явц хурдан байгаа бөгөөд дээрх 440 өвчтөний ойрын хүрээний нийт 2197 хүнд тандалт хийж, 765 хүний халдваргүйг тогтоож, 1394 хүнийг үргэлжлүүлэн хянаж байна.

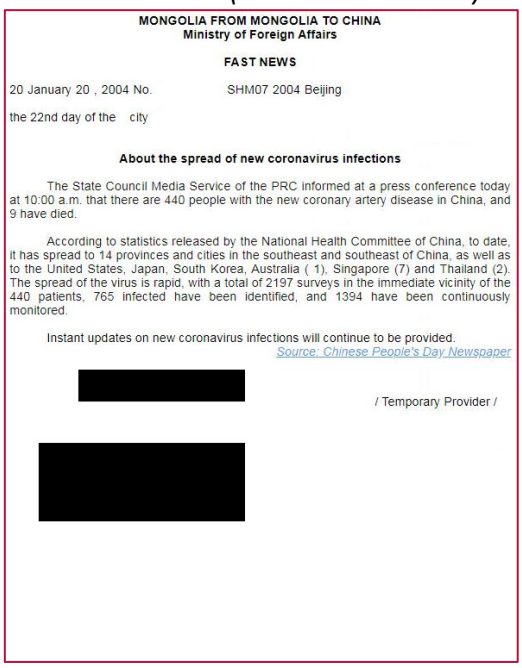
Шинэ коронавирусын халдварын талаарх шуурхай мэдээллийг үргэлжлүүлэн хүргэх болно.

Эх сурвалж: Хятадын Ардын өдрийн сонин цахим мэдээ

БОЛОВСРУУЛСАН: [redacted]

[redacted]

Traduzido (automaticamente)



MONGOLIA FROM MONGOLIA TO CHINA
Ministry of Foreign Affairs

FAST NEWS

20 January 20 , 2004 No. SHM07 2004 Beijing

the 22nd day of the city

About the spread of new coronavirus infections

The State Council Media Service of the PRC informed at a press conference today at 10:00 a.m. that there are 440 people with the new coronary artery disease in China, and 9 have died.

According to statistics released by the National Health Committee of China, to date, it has spread to 14 provinces and cities in the southeast and southeast of China, as well as to the United States, Japan, South Korea, Australia (1), Singapore (7) and Thailand (2). The spread of the virus is rapid, with a total of 2197 surveys in the immediate vicinity of the 440 patients, 765 infected have been identified, and 1394 have been continuously monitored.

Instant updates on new coronavirus infections will continue to be provided.

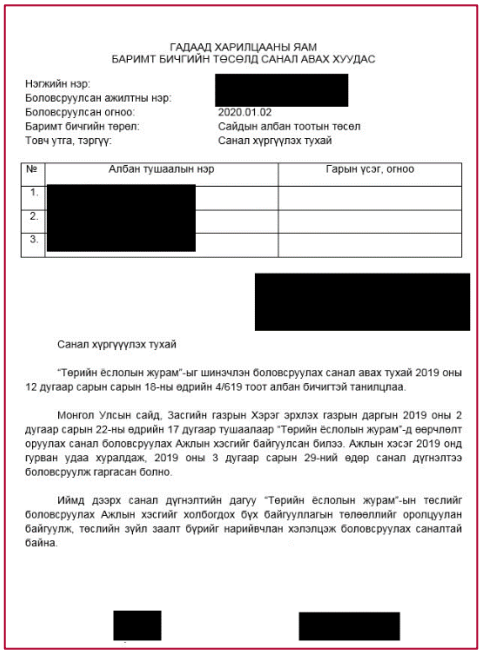
Source: Chinese People's Day Newspaper

[redacted] / Temporary Provider /

[redacted]

Documento 1: Sobre o predomínio de novas infecções por Coronavírus

Original *Traduzido (automaticamente)*



ГАДААД ХАРИЛЦААНЫ ЯАМ
БАРИМТ БИЧГИЙН ТӨСӨЛД САНАЛ АВАХ ХУУДАС

Нэгжийн нэр:
Боловсруулсан ажилтны нэр: [redacted]
Боловсруулсан огноо: 2020.01.02
Баримт бичгийн төрөл: Сайдын албан тоотын төсөл
Товч утга, тэргүү: Санал хүргүүлэх тухай

№	Албан тушаалын нэр	Гарын үсэг, огноо
1.	[redacted]	
2.		
3.		

[redacted]

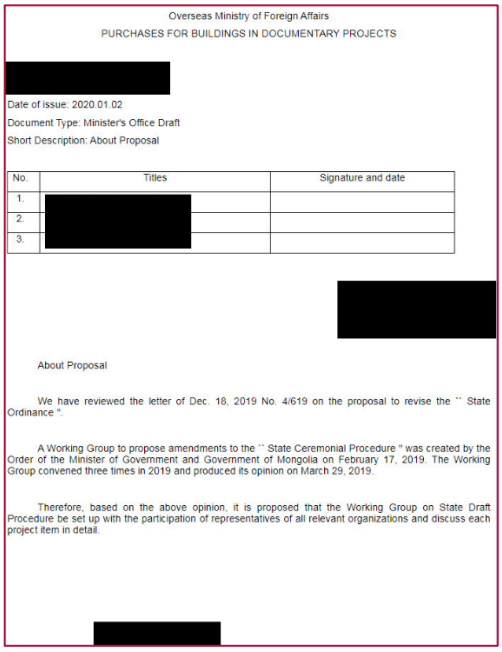
Санал хүргүүлэх тухай

"Төрийн ёслолын журам"-ыг шинэчлэн боловсруулах санал авах тухай 2019 оны 12 дугаар сарын сарын 18-ны өдрийн 4/619 тоот албан бичигтэй танилцлаа.

Монгол Улсын сайд, Засгийн газрын Хэрэг эрхлэх газрын даргын 2019 оны 2 дугаар сарын 22-ны өдрийн 17 дугаар тушаалаар "Төрийн ёслолын журам"-д өөрчлөлт оруулах санал боловсруулах Ажлын хэсгийг байгуулсан билээ. Ажлын хэсэг 2019 онд гурван удаа хуралдаж, 2019 оны 3 дугаар сарын 29-ний өдөр санал дүгнэлтээ боловсруулж гаргасан болно.

Иймд дээрх санал дүгнэлтийн дагуу "Төрийн ёслолын журам"-ын төслийг боловсруулах Ажлын хэсгийг холбогдох бүх байгууллагын төлөөллийг оролцуулан байгуулж, төслийн зүйл заалт бүрийг нарийвчлан хэлэлцэж боловсруулах саналтай байна.

[redacted] [redacted]



Overseas Ministry of Foreign Affairs
PURCHASES FOR BUILDINGS IN DOCUMENTARY PROJECTS

[redacted]

Date of issue: 2020.01.02
Document Type: Minister's Office Draft
Short Description: About Proposal

No.	Titles	Signature and date
1.	[redacted]	
2.		
3.		

[redacted]

About Proposal

We have reviewed the letter of Dec. 18, 2019 No. 4/619 on the proposal to revise the `` State Ordinance ''.

A Working Group to propose amendments to the `` State Ceremonial Procedure '' was created by the Order of the Minister of Government and Government of Mongolia on February 17, 2019. The Working Group convened three times in 2019 and produced its opinion on March 29, 2019.

Therefore, based on the above opinion, it is proposed that the Working Group on State Draft Procedure be set up with the participation of representatives of all relevant organizations and discuss each project item in detail.

[redacted]

Documento 2: COMPRAS PARA EDIFÍCIOS EM PROJETOS DOCUMENTADOS

Esses arquivos RTF foram armados usando a versão 7.x de uma ferramenta chamada RoyalRoad (também conhecida como *8.t*). Essa ferramenta, comumente usada por vários atacantes chineses, permite a criação de documentos personalizados com objetos incorporados que exploram as vulnerabilidades do Equation Editor do Microsoft Word.

Cadeia da infecção

Depois que a vítima abre o documento RTF especialmente criado e o Microsoft Word é explorado, um arquivo chamado *intel.wll* é colocado na pasta de inicialização do Word: %APPDATA%\Microsoft\Word\STARTUP.

Essa técnica de persistência é frequentemente usada por versões mais recentes do chamado *RoyalRoad*. Sempre que o aplicativo Microsoft Word é iniciado, todos os arquivos DLL com extensão *WLL* da pasta Inicialização do Word, também são iniciados, acionando a cadeia de infecção que descrita a seguir:

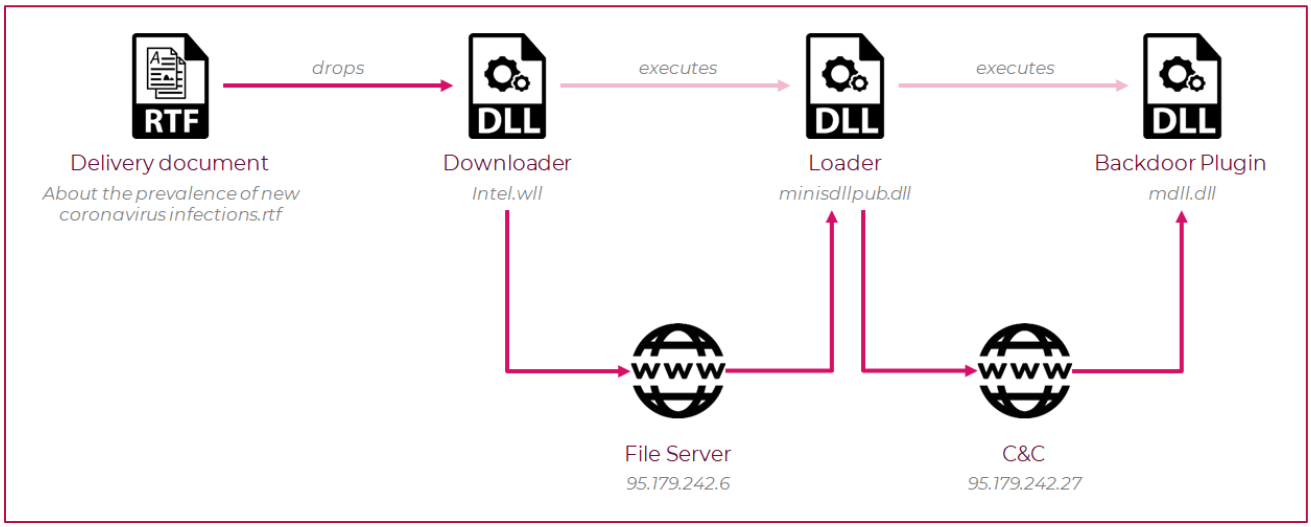


Diagrama da cadeia de infecção

Essa técnica não serve apenas como uma técnica de persistência, mas também evita que a cadeia de infecção seja totalmente detonada se for executada dentro de uma sandbox, pois é necessário um relançamento do Microsoft Word para a execução completa do malware.

Uma vez carregada, a DLL maliciosa *intel.wll* prossegue para baixar e decifrar o próximo estágio da cadeia de infecção, de um dos servidores do atacante: 95.179.242[.]6.

O próximo estágio baixado também é um arquivo DLL e é o principal carregador da estrutura de malware desenvolvida pelos atacantes. É executado usando o *Rundll32* e se comunica com outro servidor C&C do atacante (95.179.242[.]27) para receber funcionalidades adicionais.

O atacante operava o servidor C&C dentro de uma janela diária limitada, permanecendo on-line apenas por algumas horas por dia, dificultando a análise e o acesso às partes avançadas da cadeia de infecção.

No estágio final da cadeia de infecção, e quando o comando apropriado é recebido, o carregador mal-intencionado baixa e decifra um módulo RAT, novamente, na forma de um arquivo DLL, e carrega-o na memória. Essa arquitetura semelhante a um plug-in sugere a existência de outros módulos, além do payload que recebemos.

O módulo RAT parece ser um malware personalizado e exclusivo, embora possua alguns recursos bastante comuns, conforme listado abaixo:

- Fazer uma captura de tela
- Listar arquivos e diretórios
- Criar e excluir diretórios
- Mover e excluir arquivos
- Baixar um arquivo
- Executar um novo processo
- Obter uma lista de todos os serviços

Janela aberta

No início da pesquisa da Check Point, um dos servidores do atacante, que suportava o malware do estágio seguinte, tinha a listagem de diretórios ativada por um tempo limitado, permitindo o download de todos os arquivos hospedados, além de obter algumas informações sobre o cronograma da operação e os horários de trabalho dos atacantes.

Diretório aberto no servidor 95.179.242[.]6

Embora estejam disponíveis para download, todos os arquivos no servidor vieram cifrados.

Felizmente, utilizando o mesmo esquema de cifras, visto na cadeia de infecções, os pesquisadores conseguiram decifrar a maioria dos arquivos armazenados no servidor.

```
key = VkvX7CK7X7*t$x&hssLR6fOyFSaKrFJKx&@#AK*Fnukj@J9J40f1mKaN$nsCNKPe
def decrypt(enc,offset):
   decrypted =
   for i in range(len(enc)):
      decrypted += chr((ord(enc[i]) ^ ord(key[(i + offset) & 0x3f])))
   return decrypted
```

Decryption scheme derived from “intel.wll”

As dezenas de arquivos que foram possíveis de decifrar podem ser divididos em quatro grupos principais de famílias de carregadores de malware. Seus nomes internos incorporados e funcionalidade principal estão descritos abaixo:

http_dll.dll (Intel.wll)	O carregador do primeiro estágio descrito acima. Decifra o endereço C&C, baixa e decifra a DLL do próximo estágio e a executa via Rundll32.
ppdown.dll	Funciona como downloader e decodificador dos arquivos .rar armazenados no servidor do atacante. Lê um arquivo “access.txt” do servidor e decifra-o e divide o resultado em três partes: 1) O nome do próximo estágio a ser baixado. 2)

	A próxima etapa da função de exportação a ser chamada. 3) A chave para decifrar o próximo estágio.
Rundll32Templete.dll	Essa variante serve como carregador e decodificador para a carga útil do próximo estágio. A carga útil é decifrada na seção .sect.
Minisdllpub.dll	O carregador do segundo estágio, totalmente descrito abaixo. Carrega plugins DLL adicionais. Uma versão semelhante desse payload, chamada minisdllpublog.dll, contém alguns recursos adicionais de impressão de depuração.

Conexão com outras amostras

Depois de decifrar e obter acesso aos arquivos adicionais, os pesquisadores conseguiram procurar amostras semelhantes.

A busca de arquivos semelhantes pelos nomes internos (*http_dll*, *Rundll32Templete* e *minisdllpub*), funções exportadas exclusivas (*Engdic*, *WSSet* e *MSCheck*) e semelhanças de código (métodos para decodificar, padrões de comunicação etc.), permitindo encontrar mais amostras relacionadas ao atacante:

5560644578a6bcf1ba79f380ca8bdb2f9a4b40b7 **http_dll.dll**
207477076d069999533e0150be06a20ba74d5378 **http_dll.dll**
b942e1d1a0b5f0e66da3aa9bbd0fb46b8e16d71d **http_dll.dll**
9ef97f90dcdfe123ccb7d9b45e6fa9eceb2446f0 **hcc_dll.dll**
cf5fb4017483cdf1d5eb659ebc9cd7d19588d935 **Rundll32Templete.dll**
92de0a807cfb1a332aa0d886a6981e7dee16d621 **Rundll32Templete.dll**
cde40c325fcf179242831a145fd918ca7288d9dc **minisdllpublog.dll**
2426f9db2d962a444391aa3ddf75882faad0b67c **IrmonSvc.dll**
9eda00aae384b2f9509fa48945ae820903912a90 **IrmonSvc.dll**
2e50c075343ab20228a8c0c094722bbff71c4a2a **IrmonSvc.dll**
2f80f51188dc9aea697868864d88925d64c26abc **NWCWorkstation.dll**

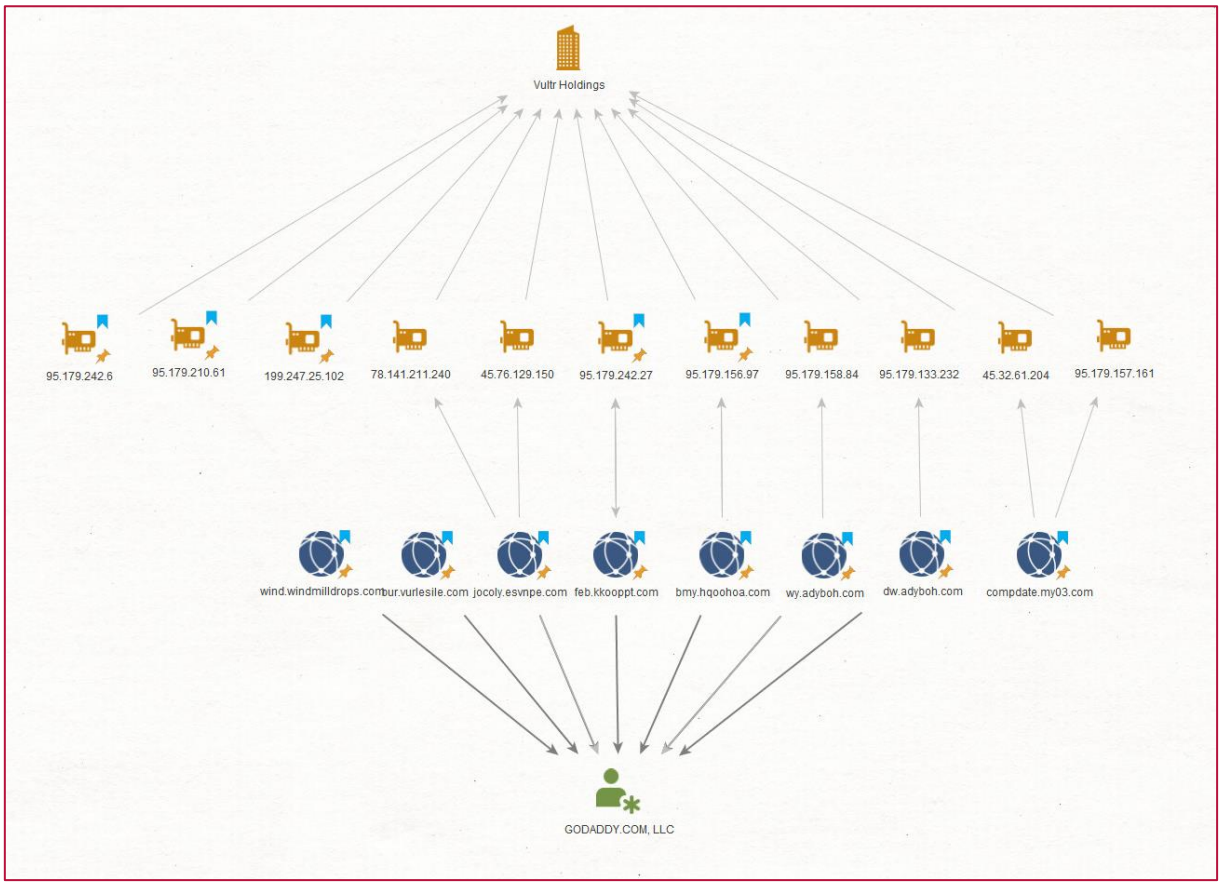
Exemplos similares encontrados

Uma das amostras encontradas (92de0a807cfb1a332aa0d886a6981e7dee16d621) levou os pesquisadores a um artigo cobrindo uma cadeia de infecção inicial semelhante que parecia perseguir alvos ucranianos.

Outra amostra (9ef97f90dcdfe123ccb7d9b45e6fa9eceb2446f0) foi originalmente descartada por um documento RTF que parecia ser alvo de entidades na Federação Russa, no final de 2018.

Infraestrutura

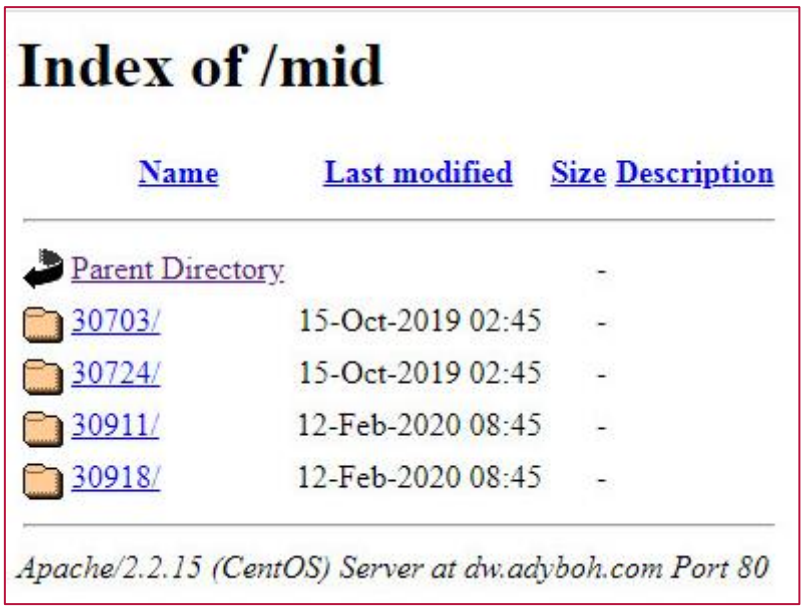
Analisar as amostras recém-descobertas revelou uma parte maior da infraestrutura utilizada pelo atacante e um TTP comum: todos os servidores da C&C estavam hospedados em servidores **Vultr** e os domínios registrados pelo registrador **GoDaddy**.



Infrastructure overview

Ao analisar esta campanha, além da infraestrutura utilizada, também foi observado um comportamento interessante dos atacantes.

Em um determinado momento, o servidor C&C 95.179.242[.]6 parou de servir a lista de diretórios abertos e, alguns dias depois, dw.adyboh[.]com tornou-se um público:



Index of /mid

Name	Last modified	Size	Description
Parent Directory		-	
30703/	15-Oct-2019 02:45	-	
30724/	15-Oct-2019 02:45	-	
30911/	12-Feb-2020 08:45	-	
30918/	12-Feb-2020 08:45	-	

Apache/2.2.15 (CentOS) Server at dw.adyboh.com Port 80

Diretório do servidor publicado em dw.adyboh[.]com

Isso pode sugerir que os atacantes estão ativando a listagem de diretórios quando um de seus servidores de entrega de payload está em uso.

Atribuição

Da perspectiva de documentos maliciosos, os pesquisadores da Check Point acreditam que a nomeação de *intel.wll*, que é eliminada pela versão 7.x do *RoyalRoad*, não é suficiente para fazer uma atribuição clara, pois foi observado o mesmo nome usado por vários atacantes eliminando malware de diferente famílias como *Bisonal* e *Poison Ivy*.

Da perspectiva de payload, uma vez que foram encontradas as amostras adicionais e relacionadas às mencionadas acima, foi possível conectá-lo a um grupo de ameaças conhecido. Na amostra NWCWorkstation.dll mencionada acima, observou-se uma sequência única como parte da funcionalidade de log: ***V09SS0lO*** - que apontou para um artigo de 2017 da Palo Alto Networks, denominado *Governo da Bielorrússia é alvo de atacantes*, utilizando um RAT chamado *BYEBY*.

O próprio artigo também se conecta a um outro anterior de 2016, no qual as mesmas ferramentas foram usadas em um ataque contra o governo da Mongólia. O artigo também explora as conexões entre esses ataques e alguns anteriores relacionados ao Trojan *Enfal*.

Ao comparar os IOCs do ataque de 2017 à essa campanha, os pesquisadores da Check Point observaram várias semelhanças:

Semelhanças de infraestrutura

Os servidores da publicação de 2017 foram configurados na mesma infraestrutura de todas as outras amostras encontradas durante a investigação da Check Point, utilizando os serviços **Vultr** e **GoDaddy**.

Semelhanças no código

Ao analisar um dos arquivos do diretório aberto (*bf9ef96b9dc8bdbc6996491d8167a8e1e63283fe*) foi notado que ele decifra e carrega uma DLL chamada *wincore.dll*. Investigando o arquivo descartado foram feitas várias correlações com a amostra *BYEBY* a partir de 2017:

1. **Semelhança de Strings**:

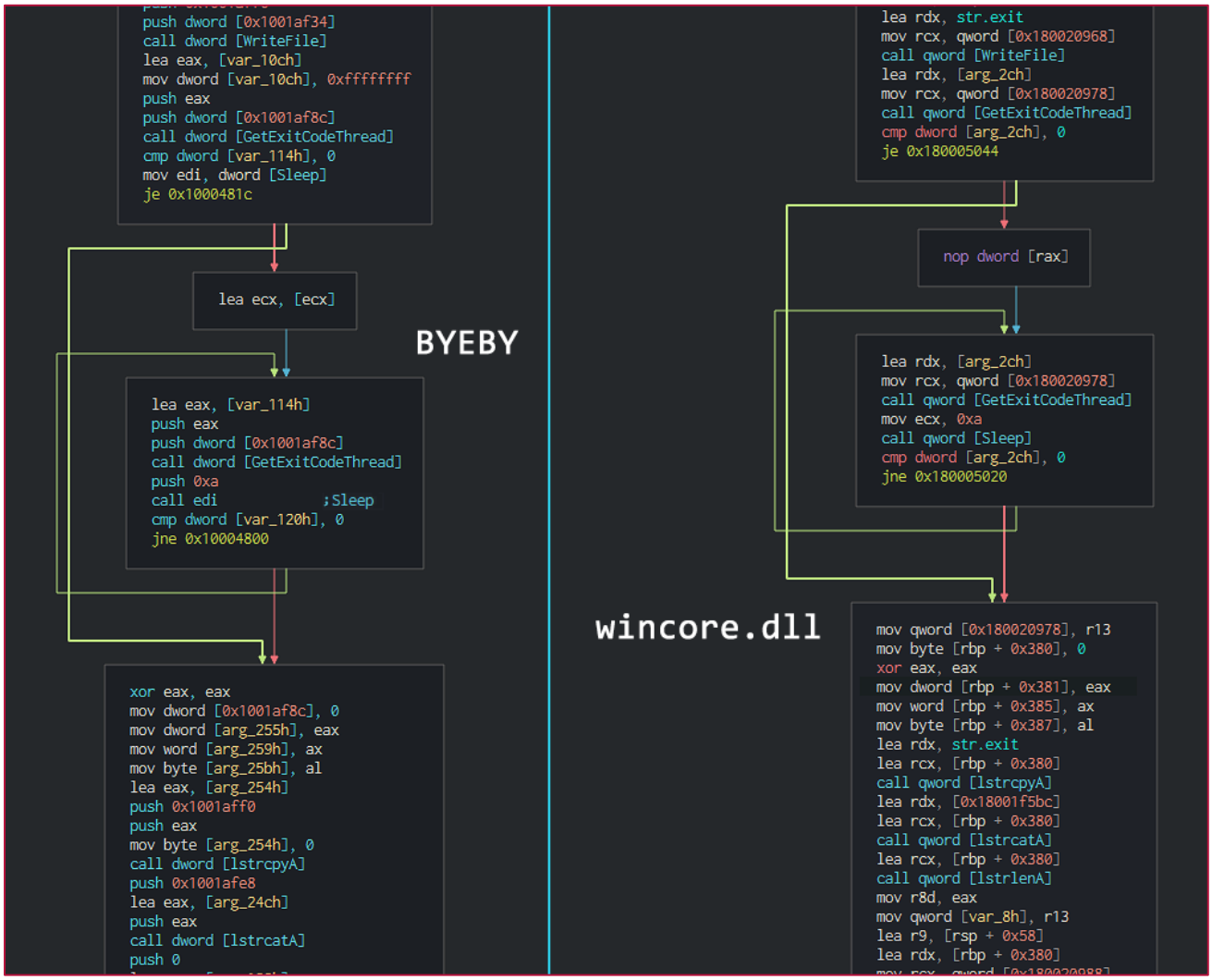
```
; CHAR pszPackage[]
pszPackage      db 'Schannel',0          ; DATA XREF: sub_10002850+1AF↑o
                                         ; StartAddress+6C4↑o
                align 10h
aWinsta0Default db 'winsta0\default',0   ; DATA XREF: StartAddress+1038↑r
headers         db 'ent-length: 0',0Dh,0Ah
                                         ; DATA XREF: sub_10001FB0+165↑r
                db 0Dh,'oxy-Connection: TP/1.1',0Dh,0Ah
                db 'Accept: %d-%d-%d %d:%d:%CONNECT %s:%d HTft\Windows\CurreGenerateG'
                db 'roupPolntVersion\InternSoftware\Microso*/*',0Dh,0Ah
                db 'Content-Type: text/html',0Dh,0Ah
                db 'Pr",SvchostPushSerKeep-Alive',0Dh,0Ah
                db 'Cont'
```

"BYEBY" strings


```
pszPackage      db 'Schannel',0          ; DATA XREF: StartAddress+9E7↑o
                align 10h
aGxvz671yvfDD   db 'GXVz671YVF%d-%d',0   ; DATA XREF: StartAddress+A2C↑r
aJcndhgwxk7SD   db 'JcNDHGwxk7%s:%d',0   ; DATA XREF: StartAddress+52E↑r
aLnboflywh8SD   db 'lnboFlywH8%s:%d',0   ; DATA XREF: StartAddress+697↑r
aU6pjqar3gqSD   db 'u6Pjqar3GQ%s:%d',0   ; DATA XREF: StartAddress+807↑r
; char *headers
headers         db 'ent-length: 0',0Dh,0Ah
                                         ; DATA XREF: sub_180001DB0+136↑r
                db 0Dh,'oxy-Connection: TP/1.1',0Dh,0Ah
                db 'Accept: CONNECT %s:%d HTft\Windows\CurrentVersion\InternSoftware\'
                db 'Microso*/*',0Dh,0Ah
                db 'Content-Type: text/html',0Dh,0Ah
                db 'PrKeep-Alive',0Dh,0Ah
                db 'Cont"'
```

“wincore.dll” strings

2. Similaridade de funções - Funções importantes no *BYEBY* e no wincore.dll quase têm a mesma implementação. Uma dessas funções é a função principal do encadeamento de payload.



Similaridades na implantação do Malware

3. Global Call-Graph e X-Ref Graph - Embora exista alguma ofuscação nos dois exemplos, foi possível verificar que eles possuem um gráfico de chamada e referência semelhante, o que significa que a funcionalidade principal dos executáveis é a mesma.

Payload - análise aprofundada

Para recapitular, a carga útil do segundo estágio na cadeia do ataque analisada é um arquivo DLL cifrado chamado *minisdllpub.dll*. A DLL, baixada de 95.179.242[.]6, é um downloader de um payload adicional. Na seção a seguir foi examinada sua implementação, destacando as características exclusivas desse payload.

O *Minisdllpub.dll* começa com a criação de um *mutex* (exclusão mútua) com o nome *Afx:DV3ControlHost*, esse é um indicador exclusivo que pode ser usado posteriormente para procurar mais amostras. Em seguida, define uma estrutura de tamanho 0x5f8 para armazenar informações do sistema e do ambiente, como o nome do computador em execução, endereços IP, nome do usuário e versão do sistema operacional. Em seguida, é criada outra estrutura do tamanho 0x3FC, desta vez para armazenar ponteiros para DLLs carregadas e funções de API, além do endereço IP da C&C (95.179.242[.]27) e porta (443).

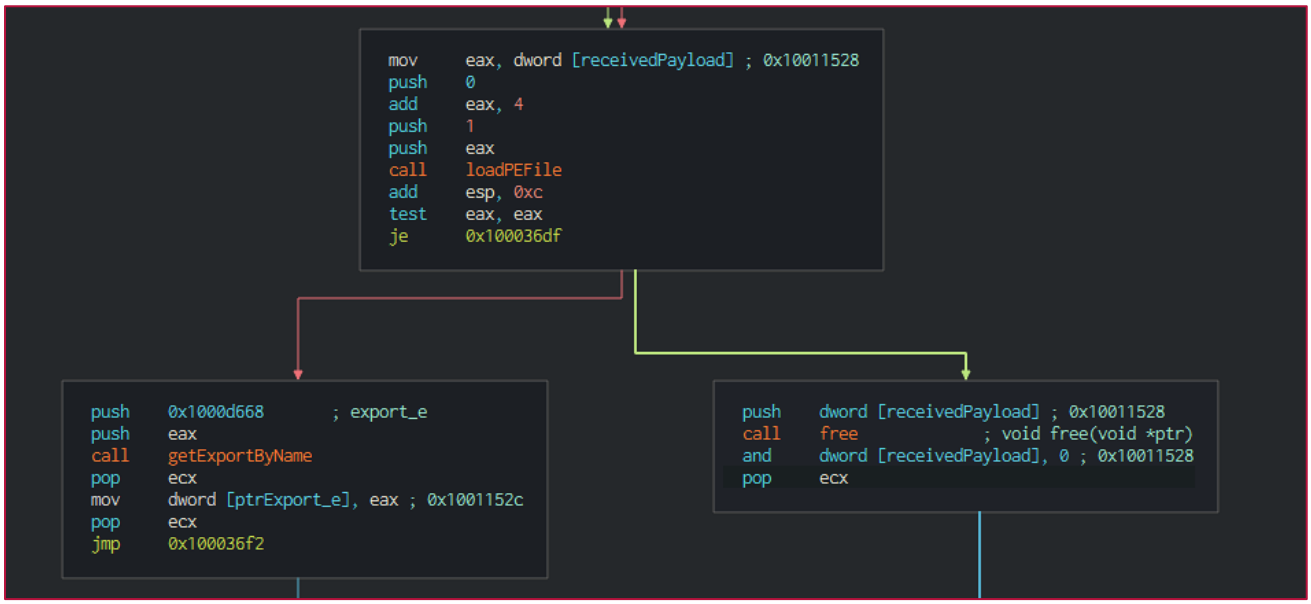
Após configurar essas estruturas, o fluxo continua e um novo encadeamento é criado. Primeiro, ele busca várias listas de funções da API e as carrega dinamicamente. Como pode ser visto na imagem a seguir, cada lista é composta por um nome de uma biblioteca seguido por uma sequência de funções da API a serem carregadas dessa biblioteca. Ponteiros para essas funções serão adicionados à estrutura anterior, que será usada para invocá-los dinamicamente quando necessário.

```
0x1000d07a      .byte 0x00
0x1000d07b      .byte 0x00
0x1000d07c          .string "POST / HTTP/1.1\r\nHost: %s\r\nContent-Length: %d\r\nCache-Control: no-cache\r\n\r\n" ; len=75
0x1000d0c7      .byte 0x00
0x1000d0c8          .string "advapi32.dll,RegCreateKeyW,RegSetValueExW,RegCloseKey,RegQueryValueExW,EnumServicesStatusExW,RegOpenKeyExW,RegQueryValueExA," ; len=125
0x1000d145      .byte 0x00
0x1000d146      .byte 0x00
0x1000d147      .byte 0x00
0x1000d148          .string "ws2_32.dll,WSAStartup,socket,connect,send,recv,closesocket,setsockopt,htons,inet_addr,gethostbyname,inet_ntoa," ; len=111
0x1000d1b7      .byte 0x00
0x1000d1b8          .string "msvcrt.dll,memcpy,memset,memcmp,sprintf,strcat,malloc,free,strstr," ; len=67
0x1000d1fb      .byte 0x00
0x1000d1fc          .string "KERNEL32.DLL,CreateFileA,ReadFile,WriteFile,SetFilePointer,CreateProcessW,TerminateProcess,OpenProcess,GetStartupInfoA,CreateEventA,OpenEv
```

Comma-separated lists of API functions, prepended with the library name

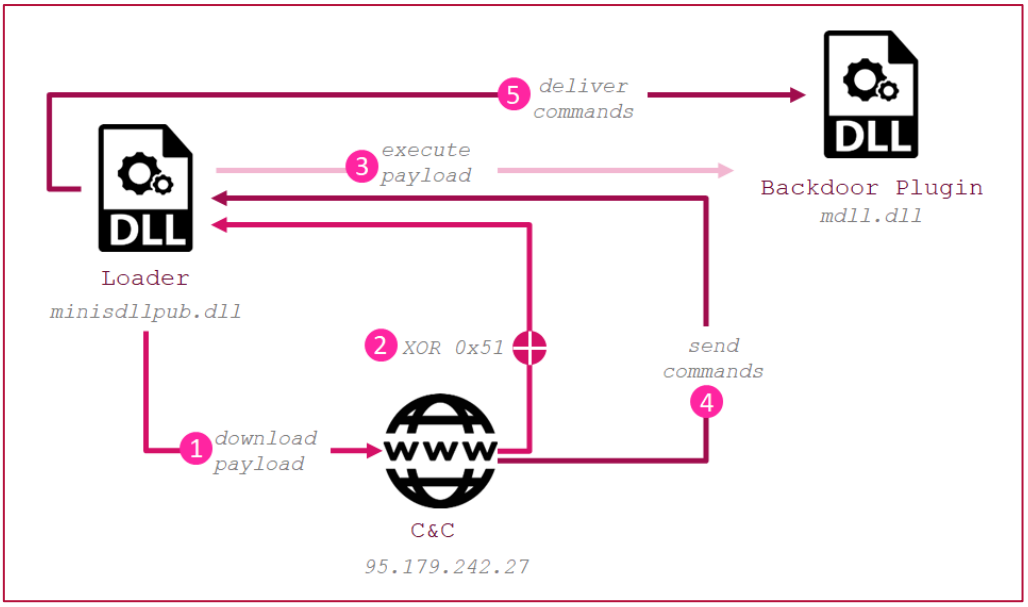
O payload do segundo estágio configura a comunicação HTTP ou HTTPS, dependente de várias verificações, e começa a se comunicar com seu C&C em novos encadeamentos. Quando o servidor responde, ele envia a DLL codificada em XOR para o malware, com a chave 0x51. O *Minisdllpub.dll* decodifica a carga útil especificada e carrega dinamicamente o novo PE na memória.

Quando carregado, ele procura uma função de exportação (export) com o nome e. O malware continua ouvindo os comandos do servidor e, quando recebidos, os passa para a função 'e' do payload recém-carregado. Ao fazer isso, o segundo estágio está operando como intermediário entre a C&C e o payload final - uma ferramenta de acesso remoto.



The malware is searching for the export function “e”, in order to invoke it

Neste ponto, temos um layout exclusivo de módulos carregados no computador da vítima. Primeiro, é o Minisdllpub.dll que foi carregado inicialmente usando o *Rundll32* por *http_dll.dll* (*intel.wll*) quando um aplicativo do Microsoft Office foi executado. Em seguida, temos o payload do RAT, que recebe seus comandos de controle não diretamente do C&C, mas, através do *Minisdllpub.dll*, que atua como mediador.



Loader execution flow

Curiosamente, além dos comandos a serem executados, o *Minisdllpub.dll* também passa várias estruturas para o payload final. As estruturas que foram construídas e preenchidas anteriormente, agora são usadas pelo RAT para chamar dinamicamente as funções da API e entregar dados ao servidor de comando e controle. Essa abordagem exclusiva de reutilizar ponteiros de função que foram carregados no módulo anterior tornará a análise do RAT dificilmente possível sem o estágio anterior.

As funcionalidades suportadas do payload final, bem como os respectivos comandos que ela recebe e envia, estão descritas na tabela que pode ser encontrada no Apêndice A abaixo.

Conclusão

Nesta campanha, a equipe da Check Point observou a mais recente repetição do que parece ser uma operação de longa data baseada na China contra uma variedade de governos e organizações em todo o mundo. Essa campanha específica estava alavancando a pandemia do COVID-19 para atrair as vítimas para desencadear a cadeia de infecção.

Os atacantes atualizaram seu conjunto de ferramentas, de documentos com macros e explorações de RTF mais antigas, para a variação mais recente do "RoyalRoad" criador de exploit de RTF amplamente utilizado.

A intenção total desse grupo chinês especializado em APT ainda é um mistério, mas eles vieram para ficar; atualizando suas ferramentas e ao que parece eles farão o que for necessário para atrair vítimas à sua rede, mesmo usando cruelmente o interesse público na atual epidemia global, se necessário.

O Check Point SandBlast Agent protege contra esse ataque do APT e é capaz de impedi-lo desde os primeiros passos.

Apêndice A: Módulo RAT - Comandos Suportados

Command ID (Sent from C&C)	Sub Command ID (Sent from C&C)	Description	Response ID (Sent from Bot)
0x21		Write a file to a specified path. Set the written file's timestamp to the timestamp of the local kernel32.dll.	0x22
0x23		Get contents of a file.	0x24
0x25		List files in a directory.	0x26
0x2E		Execute command in a new thread.	0x31
0x2F		Execute a command.	0x30
0x32	0x00	Create a directory of by a given path.	0x33
0x32	0x01	Remove a directory in a given path.	0x33
0x32	0x02	Move a file from a given path to a given directory.	0x33
0x32	0x03	Delete a file in a given path.	0x33
0x32	0x04	Move a file from a given path to a given directory. (Same as subcommand 0x02)	0x33
0x34	0x07	Get a list of all the services.	0x35
0x34	0x08	Execute a new process using WinExec.	0x35
0x34	0x09	Execute a new process. (Same as subcommand 0x08)	0x35
0x34	0x0A	Take a screenshot.	0x35
0x34	0x15	Set registry key values.	0x35
0x34	0x16	Download file from URL.	0x3A or 0x3B
0x34	0x17	Download file from URL. (Same as subcommand 0x16)	0x3A or 0x3B
0x34	0x18	Create Pipes and execute a new process.	0x3D or 0x3B

0x34	0x19	Create Pipes and execute a new process (same as 0x18).	0x3D or 0x3B
0x36		Copy the file of the current process with a ".t" extension and modify the registry.	0x37

Apêndice B: Arquivos no servidor

Internal File Name	SHA-1	Server Location
http_dll.dll	dde7dd81eb9527b7ef99ebeefa821b11581b98e0	img\0115\WRql7X
http_dll.dll	fc9c38718e4d2c75a8ba894352fa2b3c9348c3d7	bin\0612wy3\KFuGrS-code
ppdown.dll	601a08e77ccb83ffcd4a3914286bb00e9b192cd6	bin\0612wy3\KFuGrS
ppdown.dll	27a029c864bb39910304d7ff2ca1396f22aa32a2	bin\0612wy3\KFuGrS-ppd-bak
Rundll32Templete.dll	8b121bc5bd9382dfdf1431987a5131576321aefb	img\0115\CYMi0Y-bak img\0115\R7pEFv
Rundll32Templete.dll (x64)	bf9ef96b9dc8bdbc6996491d8167a8e1e63283fe	bin\test0625\CmlN0i
minisdllpub.dll	fcf75e7cad45099bf977fe719a8a5fc245bd66b8	img\0115\CYMi0Y img\0120\VIdALQ img\1224\AF9i1i
minisdllpublog.dll	0bedd80bf62417760d25ce87dea0ce9a084c163c	bin\0612wy3\KFuGrS-www bin\0617wy3\LX5sG1
gg.dll	5eee7a65ae5b5171bf29c329683aacc7eb99ee0c	bin\0612wy3\TTXk1U.rar
minisdllpub.dll	3900054580BD4155B4B72CCF7144C6188987CD31	Dropped by 8b121bc5bd9382dfdf1431987a513157632
wincore.dll	e7826f5d9a9b08e758224ef34e2212d7a8f1b728	Dropped by bf9ef96b9dc8bdbc6996491d8167a8e1e63

Apêndice C: IOCs adicionais

Servers:

95.179.242[.]6
95.179.242[.]27
199.247.25[.]102
95.179.210[.]61
95.179.156[.]97
dw.adyboh[.]com
wy.adyboh[.]com
feb.kkooppt[.]com
compdate.my03[.]com
jocoly.esvnpe[.]com
bmy.hqoohoa[.]com
bur.vueleslie[.]com
wind.windmilldrops[.]com

RTFs:

234a10e432e0939820b2f40bf612eda9229db720
751155c42e01837f0b17e3b8615be2a9189c997a
ae042ec91ac661fdc0230bdddaafdc386fb442a3
d7f69f7bd7fc96d842fcac054e8768fd1ecaa88a
dba2fa756263549948fac6935911c3e0d4d1fa1f

DLLs:

0e0b006e85e905555c90dfc0c00b306bca062e7b
dde7dd81eb9527b7ef99ebeefa821b11581b98e0
fc9c38718e4d2c75a8ba894352fa2b3c9348c3d7

601a08e77ccb83ffcd4a3914286bb00e9b192cd6
27a029c864bb39910304d7ff2ca1396f22aa32a2
8b121bc5bd9382dfdf1431987a5131576321aefb
bf9ef96b9dc8bdbc6996491d8167a8e1e63283fe
fcf75e7cad45099bf977fe719a8a5fc245bd66b8
0bedd80bf62417760d25ce87dea0ce9a084c163c
5eee7a65ae5b5171bf29c329683aacc7eb99ee0c
3900054580BD4155B4B72CCF7144C6188987CD31
e7826f5d9a9b08e758224ef34e2212d7a8f1b728
a93ae61ce57db88be52593fc3f1565a442c34679
5ff9ecc1184c9952a16b9941b311d1a038fcab56
36e302e6751cc1a141d3a243ca19ec74bec9226a
080baf77c96ee71131b8ce4b057c126686c0c696
c945c9f4a56fd1057cac66fbc8b3e021974b1ec6
5560644578a6bcf1ba79f380ca8bdb2f9a4b40b7
207477076d069999533e0150be06a20ba74d5378
b942e1d1a0b5f0e66da3aa9bbd0fb46b8e16d71d
9ef97f90dcdfe123ccb7d9b45e6fa9eceb2446f0
cf5fb4017483cdf1d5eb659ebc9cd7d19588d935
92de0a807cfb1a332aa0d886a6981e7dee16d621
cde40c325fcf179242831a145fd918ca7288d9dc
2426F9DB2D962A444391AA3DDF75882FAAD0B67C
9eda00aae384b2f9509fa48945ae820903912a90
2e50c075343ab20228a8c0c094722bbff71c4a2a
2f80f51188dc9aea697868864d88925d64c26abc

RAT:

238a1d2be44b684f5fe848081ba4c3e6ff821917

