BOLETIM DE SEGURANÇA

Campanha do Malware DarkGate

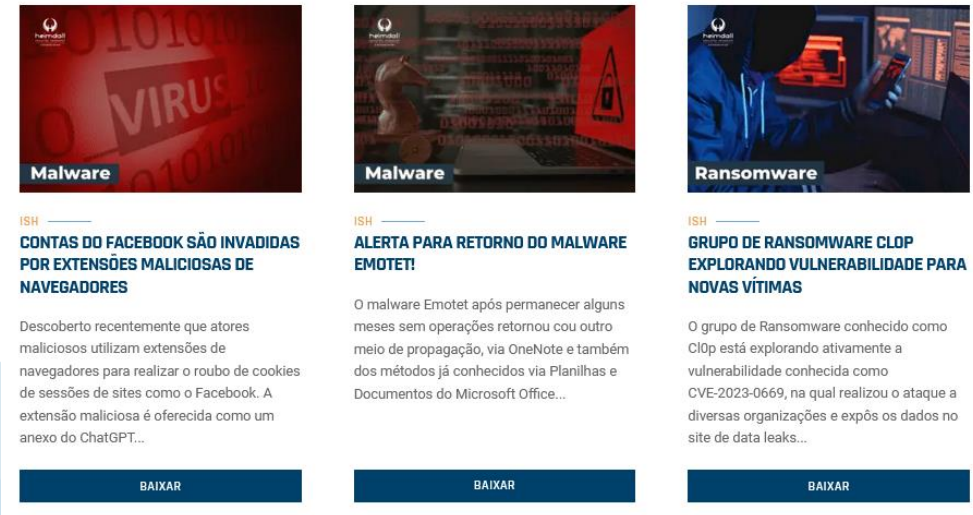
heimdall
security research
A DIVISION OF ISH

Receba alertas e informações sobre segurança cibernética e ameaças rapidamente, por meio do nosso Twitter.

Heimdall Security Research

Acesse boletins diários sobre agentes de ameaças, *malwares*, indicadores de comprometimentos, TTPs e outras informações no *site* da ISH.

Boletins de Segurança – Heimdall



heimdall
security research

Sumário

Lista de Tabelas

Lista de Figuras

1 SUMÁRIO EXECUTIVO

A equipe de Inteligência da ISH, coletou informações sobre um malware documentado e identificado pela primeira vez em 2018 conhecido e apelidado como **DarkGate** (também conhecido como MehCrypter).

Este malware é o *loader* de commodities com recursos que incluem a capacidade de baixar e executar arquivos na memória, incluindo um módulo *Hidden Virtual Network Computing (HVNC)*, *keylogging*, roubo de informações e escalonamento de privilégios. O malware utiliza arquivos AutoIT legítimos e normalmente executa vários scripts.

Além disso, foi identificado que novas versões do malware DarkGate estaria sendo anunciado em um fórum Russo desde maio de 2023.

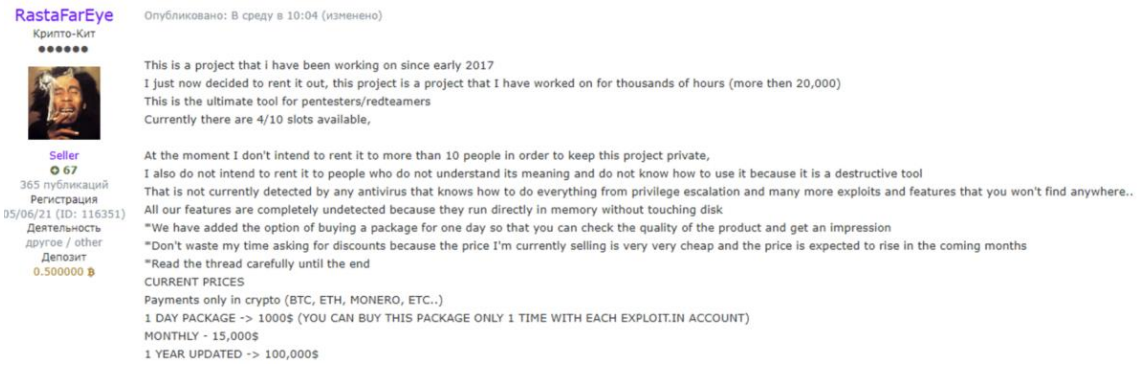


Figura 1 – Captura de tela realizada pela equipe de pesquisa ZeroFox.

Portanto, a ISH realizou a coleta de informações e compilou estas neste alerta, visando compartilhar detalhes da operação deste malware contra sistemas informáticos.

2 INFORMAÇÕES COLETADAS

Em junho, um ator de ameaça com o nome **"RastaFarEye"** teria anunciado um malware multifuncional apelidado de **DarkGate** em um fórum da Deep Web conhecido como "Exploit". O malware teria sido desenvolvido de forma privada e permitia que os agentes de ameaças construíssem as suas próprias botnets.

O malware possuía **recursos adicionais** como:

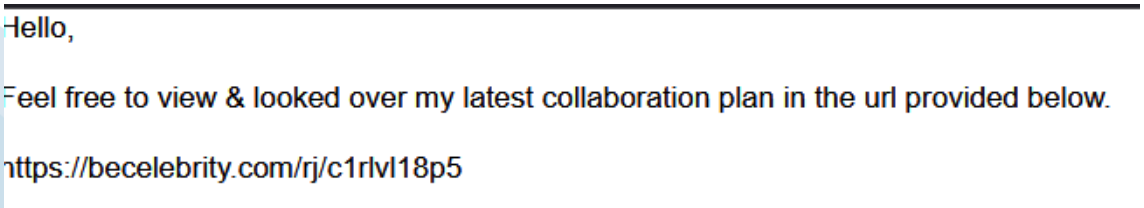
- Geração de arquivos .lnk maliciosos
- Tamanho do arquivo pequeno (490kb)
- Execução na memória do sistema
- Ofuscação de payloads para evitar a detecção pelas verificações dinâmicas da maioria dos produtos antivírus.
- Mantém o acesso às máquinas comprometidas durante as reinicializações do sistema.
- Rouba dados confidenciais de navegadores da web.
- Registra as teclas digitadas.
- Obtém permissões de nível superior em máquinas comprometidas
- Utilização dos recursos da máquina comprometida para mineração de criptomoedas.

Além disso, o **preço da licença** do malware pode variar:

- US$100.000 por ano
- US$15.000 por mês
- US$1.000 por dia

Com base em pesquisas, foi possível identificar que o malware DarkGate estaria sendo distribuído com amplas campanhas de phishing, terminando com a implantação do malware como forma de *loader*.

De acordo com relatórios tornados públicos de incidente de segurança, foi possível identificar que o malware DarkGate estaria sendo distribuído por meio de campanhas de phishing.


Hello,

Feel free to view & looked over my latest collaboration plan in the url provided below.

https://becelebrity.com/rj/c1rlvl18p5

Figura 2 – Campanha de phishing para distribuir o malware identificado pelo pesquisador 0xToxin.

Além da campanha, outra campanha observada pela AON foi publicada, na qual pode verificar que ambas as campanhas utilizaram um arquivo .MSI (Microsoft Software Installer) para propagação do malware.

Primeiro, vamos focar na análise publicada pelo pesquisador 0xToxin, na qual identificou que era realizado o download do arquivo **"Project_[0-9]{7}\.msi"**.

O arquivo baixado continha dois arquivos incorporados:

- CustomAction.dll
- WrappedSetupProgram.cab

A DLL é chamada pelo MSI para descompactar o conteúdo armazenado em WrappedSetupProgram.cab e executá-lo.

O arquivo **.cab** inclui dois arquivos:

- Autoit3.exe
- UGtZgHHT.au3 (scripts AutoIT)

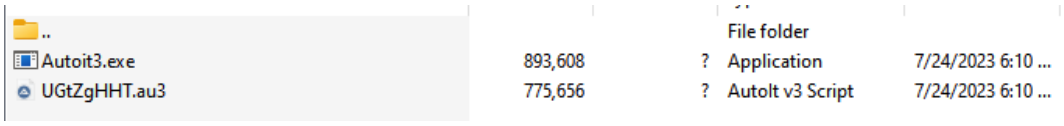


Figura 3 – Arquivos .cab relacionados ao arquivo extraído.

O arquivo script AutoIT identificado começava com os magic bytes: `A3 48 4B BE` e `41 55 33 21 45 41` (AU3!EA).

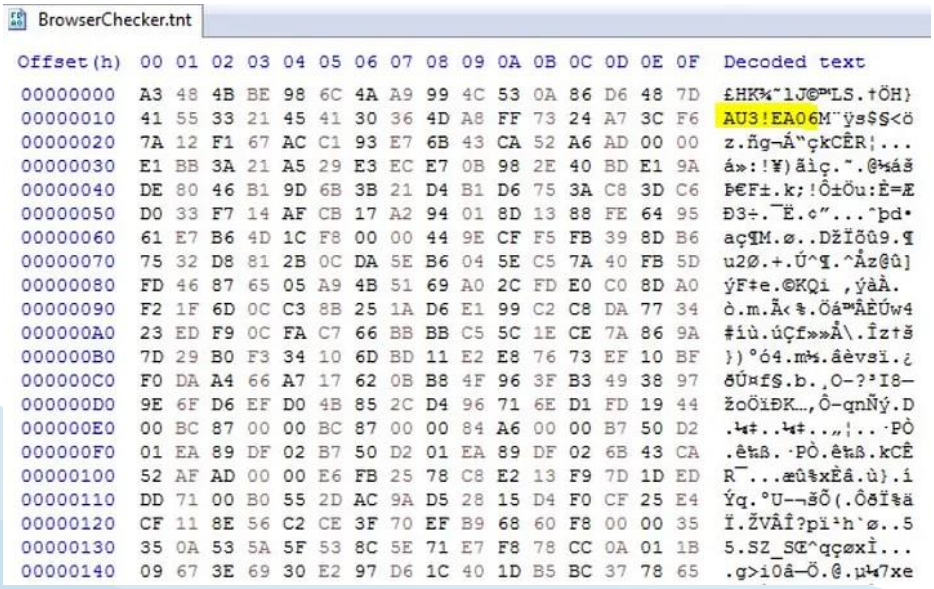


Figura 4 – magic bytes do arquivo de script AutoIT.

No script analisado pelo pesquisador foi observado uma quantia substancial de dados que pareciam ser inúteis, sendo localizado os magic bytes após a quantidade de dados aparentemente inúteis.

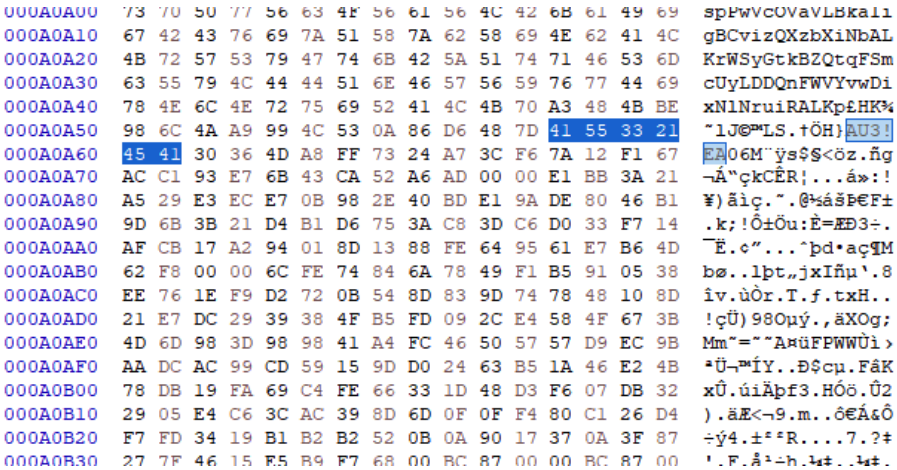


Figura 5 – magic bytes do arquivo de script AutoIT identificado.

O script AU3 consistia em dois componentes principais:

1. Um *shellcode* segmentado com codificação hexadecimal que é concatenado em uma única variável.
2. Injeção e execução do *shellcode*.

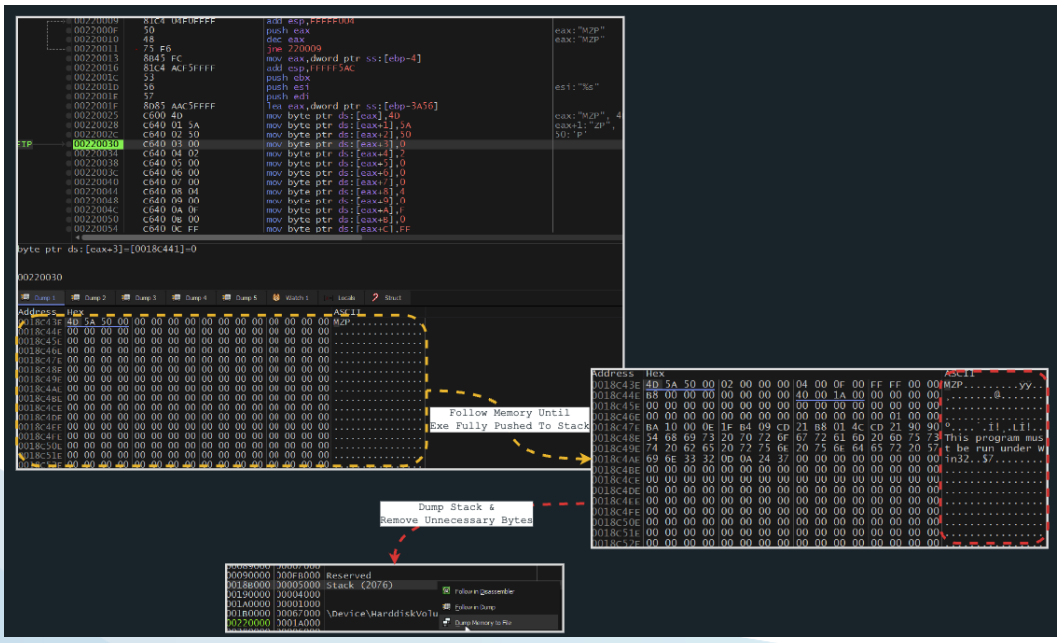


Figura 6 – Despejo do arquivo .exe (MZP) malicioso correspondente ao Loader.

O foco do pesquisador foi em identificar as strings relacionadas ao **Comando e Controle (C2)** utilizados pelos atores de ameaças. Algumas strings decodificadas pelo pesquisador apresentou algumas mensagens de notificações enviadas ao C2, como:

- New Bot: DarkGate is inside hAnyDesk user with admin rights
- DarkGate not found to get executed on the new hAnyDesk Desktop, Did you enabled Startup option on builder?
- Credentials detected, removing them!

Inclusive, a lista contendo todas as strings possíveis identificadas e decodificadas aqui. Incluindo o canal de C2 utilizado na análise do DarkGate: **http[:]//80.66.88[.]145.**

Portanto, é possível observar que o malware utilizada codificação em **base64** para ofuscação das strings, sendo publicado um script IDAPython para auxiliar na identificação das strings ofuscadas pelo malware.

3 Conclusão

Com base nas informações coletadas, a campanha utilizada como forma global utiliza threads de e-mails para phishing, levando o usuário a download do malware sofisticado como o DarkGate.

Os usuários que baixaram o malware receberam um arquivo MSI com dois arquivos incorporados que carregaram o *shellcode* codificado para execução, sendo que o DarkGate também utilizou decodificação exclusiva para duas strings incorporadas, relevando comandos enviados ao C2 e a configuração do malware.

Algumas técnicas de ofuscação como "Loop XOR" e decodificação Base64 personalizada foi observada nas atividades de rede.

4 RECOMENDAÇÕES

Além dos indicadores de comprometimento elencados abaixo pela ISH, poderão ser adotadas medidas visando a mitigação da infecção do referido *malware*, como por exemplo:

- Seja desconfiado de todos os e-mails, mensagens de texto e telefonemas. Não clique em links ou abra anexos em e-mails de remetentes desconhecidos.
- Verifique o endereço de e-mail do remetente. Os e-mails de phishing geralmente vêm de endereços de e-mail que parecem legítimos, mas podem ter pequenas diferenças, como uma letra trocada ou um domínio diferente.
- Preste atenção aos erros de ortografia e gramática. Os e-mails de phishing geralmente contêm erros de ortografia e gramática, o que pode ser um sinal de que o e-mail não é legítimo.
- Não se apresse em fornecer informações. Se você receber um e-mail que solicite informações confidenciais, não as forneça até ter certeza de que o e-mail é legítimo.
- Use um antivírus atualizado. Um antivírus atualizado pode ajudar a proteger seu computador contra malware, que às vezes é usado em ataques de phishing.
- Use uma senha forte e única para cada conta. Isso tornará mais difícil para os cibercriminosos invadirem suas contas.
- Atualize seu software regularmente. As atualizações de software geralmente incluem correções de segurança que podem ajudar a proteger seu computador contra ameaças.
- Esteja ciente das últimas tendências em ataques de phishing. Os cibercriminosos estão constantemente desenvolvendo novas técnicas de phishing, por isso é importante estar ciente das últimas tendências para que você possa se proteger.

5 IoCs

A ISH Tecnologia realiza o tratamento de diversos indicadores de compromissos coletados por meio de fontes abertas, fechadas e também de análises realizadas pela equipe de segurança Heimdall. Diante disto, abaixo listamos todos os Indicadores de Compromissos (IOCs) relacionadas a análise do(s) artefato(s) deste relatório.

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	793c0217717b0a37794f7c3adbeda577
sha1:	613a0158629bd9cdcbae1fe411358161645d8a69
sha256:	fadabbf0ef32b7295b5c0dc1830816c35bce50ec9256d01a600d06f346a161d7
File name:	eeabfcb.au3

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	e0d96c0fdcd06ab07d66a11b57a0c6ce
sha1:	d0d59ce7c7a5845100e05d899c90267a7c97356a
sha256:	5b17e978c2ca2cf03e4ffff1e4609f2ec98738b1541fa41ba5b67f061e9e2af2
File name:	darkgate.exe

Indicadores de compromisso de artefato malicioso/ analisado	
md5:	fcdc5fa36481d5ace7fa8fc40696ce71
sha1:	dafa96f73f382714fd961f7e399adc2e84f2e751
sha256:	e5ca3a8732a4645de632d0a6edfaf064bdd34a4824102fbc2b328a974350db8f
File name:	651e4a.msi

Indicadores de compromisso de artefato AutoIT	
md5:	78cdadec900811f098b6613495188391
sha1:	b4825b49943f804e5ff9a52d7c661f6c6b345b3f
sha256:	2caa6b5e92ad4c772166860d428d388a4fa376c5adc439b10ee2f045e0a1b003
File name:	files.cab

Indicadores de compromisso de artefato AutoIT	
md5:	856a0bb9b1ebc86a05a2b3367d9cbdd7
sha1:	74da333bcec76419015d7a246b1270cdc1a16e00
sha256:	206042ec2b6bc377296c8b7901ce1a00c393df89e7c4cbbb1b8da1a86a153b67
File name:	65d7c7.msi

Indicadores de compromisso de artefato AutoIT	
md5:	0d813ff082d1f7f3169876e6e58a3de7
sha1:	8bace9b1d0dc3e8d42303f08df2255b67bd07a5b
sha256:	9fd66fbc01bdd8a13ca5a8c41a235c6714e9077a269e65697723c2ab8a775501
File name:	files.cab

Indicadores de compromisso de artefato AutoIT	
md5:	c56b5f0201a3b3de53e561fe76912bfd
sha1:	2a4062e10a5de813f5688221dbeb3f3ff33eb417
sha256:	237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d
File name:	Autoit3.exe

Indicadores de compromisso de artefato AutoIT	
md5:	b2d5a1369b5b88c18e5123b948683ba8
sha1:	7f537f5045e5e4b77ccb8dcfbd04555b85b11821
sha256:	9a7db0204847d26515ed249f9ed577220326f63a724a2e0fb6bb1d8cd33508a3
File name:	angry_win_0.47_installer.msi

Indicadores de compromisso de artefato AutoIT	
md5:	3cc9a831ae0eb2f227f5f3edd1c55e26
sha1:	014f7fa81d9cbb6c4c6334186e44114815f265ee
sha256:	b6116bcb942a2e13f050417952477e7c8564cc4fd1c4c4b57a67b142b009ab6b
File name:	files.cab

Indicadores de compromisso de artefato AutoIT	
md5:	c56b5f0201a3b3de53e561fe76912bfd
sha1:	2a4062e10a5de813f5688221dbeb3f3ff33eb417
sha256:	237d1bca6e056df5bb16a1216a434634109478f882d3b1d58344c801d184f95d
File name:	Autoit3.exe

Indicadores de compromisso de artefato malicioso/ analisado	
sha256:	8137e72db1c4ef3f375378d62a7dd84c5852a9371edd87f7b2a527609f2553b8

Indicadores de compromisso de artefato malicioso/ analisado	
sha256:	457767a1726bbc1af05175b5a61612a4e1ad29d633e32a887e241acced72a006

Tabela 1 – Indicadores de Compromissos.

URLs de distribuição e endereços IP C2:

http[:]//80.66.88[.]145
107[.]181.161.200
advancedscanner[.]link
ipadvancedscanner[.]com
185.224.137[.]54
185.11.61[.]65
top[.]advscan[.]com
advanced-ips-scanne[.]com
a4scan[.]com
advanced-ip-scanne[.]com
80.66.88[.]145
107.181.161[.]200

Tabela 2 – Indicadores de Compromissos de Campanhas de Rede

6 REFERÊNCIAS

- **Heimdall *by* ISH Tecnologia**
- **Identificação da venda do malware pela ZeroFox**
- **Publicação realizada pelo AON sobre DarkGate**
- **Publicação do pesquisador 0xToxin sobre DarkGate**
- **Campanha analisada pela MalwareBytesLabs**

heimdall
security research
A DIVISION OF ISH