McAfee
An Intel Company

Resumo executivo

Desvendando o mundo do cavalo de Troia Citadel

Por Ryan Sherstobitoff
McAfee Labs

O malware "bancário" Zeus e suas variantes têm figurado nas manchetes dos últimos meses. Uma das variantes, o cavalo de Troia Citadel, ganhou notoriedade com a notícia de sua retirada do mercado aberto de crimeware. Contudo, essa retirada não significa necessariamente que o Citadel deixará de ser uma ameaça global significativa. Pesquisas do McAfee Labs determinaram que os desenvolvedores originais do Citadel, e talvez outros, estão desenvolvendo novas variantes que estendem significativamente a funcionalidade e o perfil de ameaça do Citadel.

As principais tendências observadas no segundo semestre de 2012 e no início de 2013 foram as seguintes:

- Ataques direcionados contra empresas públicas e privadas, principalmente na Europa
- Aperfeiçoamentos funcionais utilizados para roubar informações, bem como dinheiro
- Restrição de alvos a algumas centenas, em vez das dezenas de milhares de alvos observadas em utilizações anteriores da família de malware Zeus
- Coleta de credenciais de aplicativos internos, aplicativos de sistemas bancários, sistemas de manufatura, etc. que podem ser utilizados em ataques posteriores contra esses aplicativos
- Surgimento do "Poetry Group" como principal executor de ataques com base no Citadel

Foco geográfico

Ao contrário da maioria dos ataques de malware, as variantes recentes do Citadel atingiram um alvo geográfico surpreendentemente pequeno, com mais de 90% dos alvos conhecidos situados na Europa. No entanto, mesmo dentro do cenário europeu, os alvos se concentraram no norte da Europa e na Espanha, conforme mostrado na Figura 1.

Figura 1. Proliferação do Citadel na Europa.

Além disso, nossos dados de telemetria evidenciam que as quadrilhas que utilizam o Citadel não estão visando consumidores em geral. Em vez disso, os alvos são empresas e órgãos governamentais.

Extensões funcionais

A plataforma de malware Zeus foi originalmente desenvolvida para roubar dinheiro, frequentemente em pequenas quantidades, de milhares de vítimas. Contudo, os desenvolvedores do Citadel evidentemente reconheceram que dados, principalmente dados de credenciais de autenticação, podem ser mais valiosos que dinheiro. Consequentemente, no segundo semestre de 2012 começamos a ver variantes do Citadel desenvolvidas para penetrar infraestruturas de TI de grandes empresas privadas e governos locais.

O Poetry Group, que se distingue por incorporar fragmentos de poesias em inglês arcaico em suas variantes do Citadel, tem atuado ativamente em ataques contra grandes empresas privadas, conforme mostrado na Figura 2. Ataques contra alvos do setor público são mais pronunciados na Polônia, onde o Citadel tem sido utilizado para penetrar repositórios de dados de governos municipais e locais. Os pesquisadores do McAfee Labs também descobriram novas funcionalidades de fraude financeira embutidas no Citadel, escritas inteiramente em JavaScript, que parecem visar funcionários das agências do setor público sob ataque.

Variantes do Citadel distribuídas recentemente agora possuem recursos que vão além de simples fraude bancária. O malware pode coletar qualquer coisa do PC de uma vítima. O Citadel versão 1.3.45, "Extreme Edition", contém uma funcionalidade que possibilita uma conexão de controle remoto simplificado com a vítima. Em outras palavras, o cavalo de Troia estabelece (automaticamente, se necessário) a partir do painel de controle um canal oculto de comunicação com o PC da vítima. A versão 1.3.45 também tem um recurso que estabelece automaticamente uma conexão remota com redes de bots que estejam on-line, possibilitando criar scripts de ataque contra alvos diferentes. As variantes do Citadel descobertas mais recentemente também possuem uma funcionalidade própria de redirecionamento de DNS que impede que os sistemas infectados contactem os sites dos principais fornecedores de segurança de TI e autoridades policiais globais.

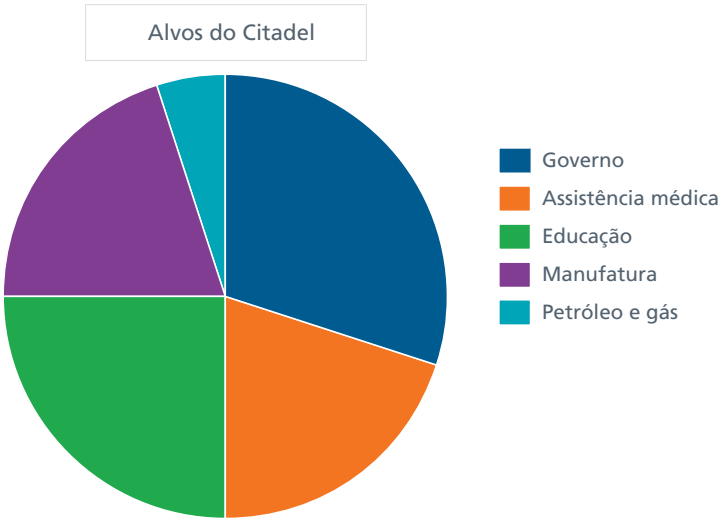

Figura 2: Alvos do Poetry Group por setor de indústria.

Volume de alvos reduzido

A grande maioria dos ataques globais de malware baseia-se na "lei dos grandes números" para ter êxito. A teoria básica é que, atacando alvos suficientes, você eventualmente encontra um número suficiente de alvos vulneráveis dos quais extrair dinheiro ou informações de interesse. Os ataques recentes do Citadel seguiram uma abordagem oposta.

Em um ataque do Citadel observado entre 22 de dezembro de 2012 e 6 de janeiro de 2013, a telemetria do McAfee Labs identificou um total de 156 vítimas em apenas quatro países, conforme mostrado na Figura 3.

País	Número de vítimas infectadas
Polônia	71
Dinamarca	44
Suécia	29
Espanha	12

Figura 3. Alvos da campanha n°1 do Citadel por país.

Poetry Group

O mais ativo dos grupos por trás de ataques com base no Citadel é conhecido como Poetry Group. Esse grupo incorpora fragmentos de texto um tanto poéticos escritos em inglês arcaico nos binários do Citadel utilizados nos ataques. Essa característica tem sido encontrada de maneira consistente nos binários, contendo determinados parágrafos de texto que aparecem na memória associada à execução do processo malicioso. Esses fragmentos não aparecem em outras campanhas observadas na Europa. Portanto, podemos determinar que um grupo específico está por trás dessas campanhas. Quando uma das variantes utilizadas em uma campanha ativa menciona a Dinamarca especificamente, Dinamarca é um dos países visados pelo ataque.

Conclusão

O Citadel é considerado uma ameaça emergente não apenas para a indústria de serviços financeiros, mas também para outras indústrias. O Citadel proporciona aos cibercriminosos uma conectividade remota avançada, e isso lhes dá a capacidade de decidir dinamicamente qual alvo atacar.

Embora o Citadel esteja sendo retirado do mercado aberto, o McAfee Labs acredita que variantes sucessoras continuarão a ser distribuídas ao longo de 2013. Também prevemos que seus alvos se expandirão conforme mais cibercriminosos perceberem que as capacidades potenciais do Citadel vão muito além da fraude financeira. Há uma quantidade significativa de atividades recentes que sugere que os executores continuarão a utilizar o Citadel para atacar empresas e organizações governamentais globalmente.

Uma cópia do relatório completo pode ser encontrada aqui:
www.mcafee.com/us/resources/white-papers/wp-citadel-trojan.pdf.

McAfee
An Intel Company

McAfee do Brasil Comércio de Software Ltda.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.mcafee.com/br

60028exs_citadel-trojan_0113_fnl_ETMG