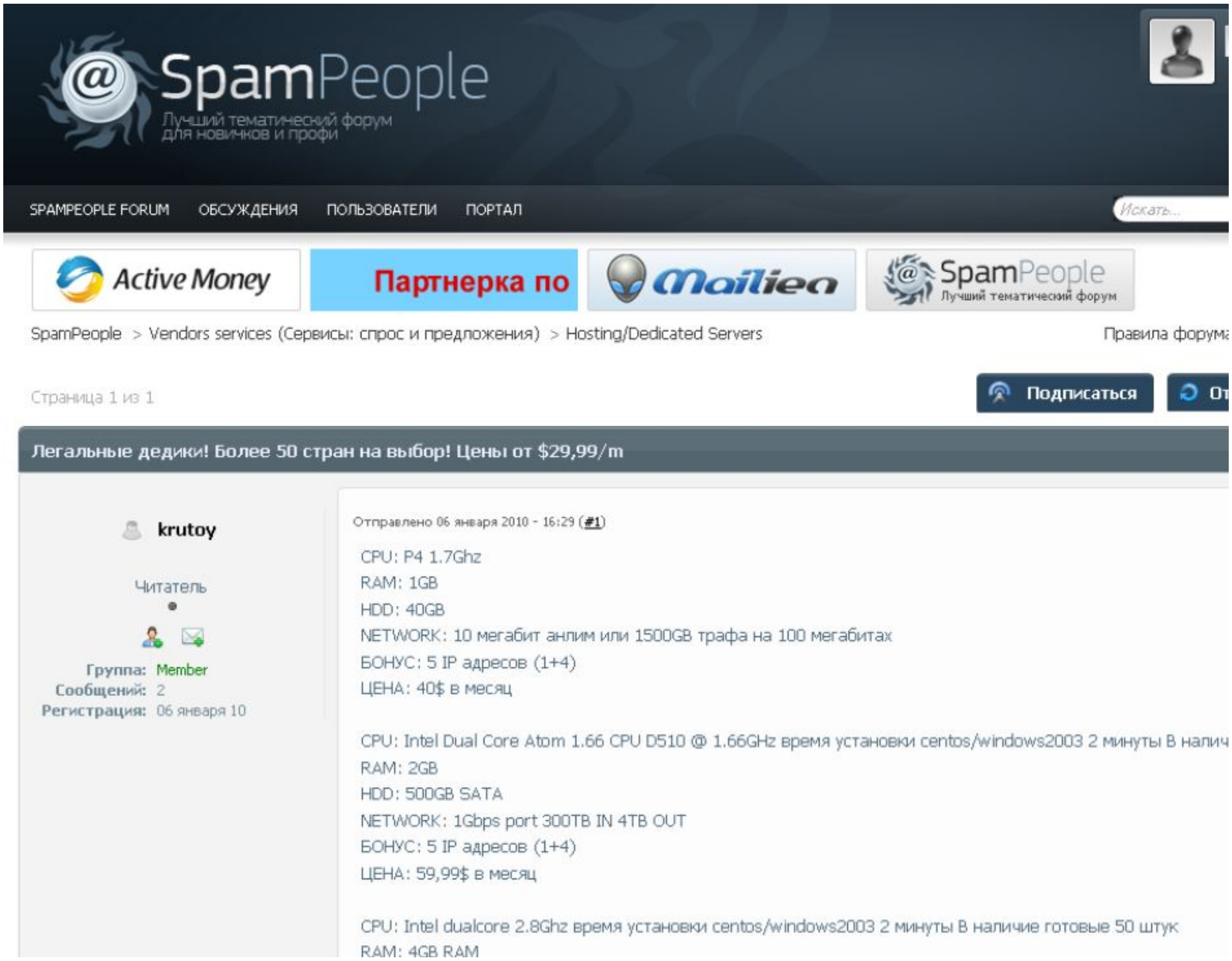
Microsoft Hunting Rustock Controllers

krebsonsecurity.com/2011/03/microsoft-hunting-rustock-controllers/


SpamPeople
Лучший тематический форум для новичков и профи
SPAMPEOPLE FORUM
ОБСУЖДЕНИЯ
ПОЛЬЗОВАТЕЛИ
ПОРТАЛ
Искать...
Active Money
Партнерка по
Mailien
SpamPeople Лучший тематический форум
SpamPeople > Vendors services (Сервисы: спрос и предложения) > Hosting/Dedicated Servers
Правила форума
Страница 1 из 1
Подписаться
От

Легальные дедики! Более 50 стран на выбор! Цены от $29,99/m

krutoy

Читатель

Группа: Member
Сообщений: 2
Регистрация: 06 января 10

Отправлено 06 января 2010 - 16:29 (#1)

CPU: P4 1.7Ghz
RAM: 1GB
HDD: 40GB
NETWORK: 10 мегабит анлим или 1500GB трафа на 100 мегабитах
БОНУС: 5 IP адресов (1+4)
ЦЕНА: 40$ в месяц

CPU: Intel Dual Core Atom 1.66 CPU D510 @ 1.66GHz время установки centos/windows2003 2 минуты В налич
RAM: 2GB
HDD: 500GB SATA
NETWORK: 1Gbps port 300TB IN 4TB OUT
БОНУС: 5 IP адресов (1+4)
ЦЕНА: 59,99$ в месяц

CPU: Intel dualcore 2.8Ghz время установки centos/windows2003 2 минуты В наличие готовые 50 штук
RAM: 4GB RAM

Who controlled the Rustock botnet? The question remains unanswered: Microsoft's recent takedown of the world's largest spam engine offered tantalizing new clues to the identity and earnings of the Rustock botmasters. The data shows that Rustock's curators made millions by pimping rogue Internet pharmacies, but also highlights the challenges that investigators still face in tracking down those responsible for building and profiting from this complex crime machine.

Earlier this month, Microsoft crippled Rustock by convincing a court to let it seize dozens of Rustock control servers that were scattered among several U.S.-based hosting providers. Shortly after that takedown, I began following the money trail to learn who ultimately paid the botnet controllers' hosts for their services.

According to interviews with investigators involved in the Rustock takedown, approximately one-third of the control servers were rented from U.S. hosting providers by one entity: A small business in Eastern Europe that specializes in reselling hosting services to shadowy individuals who frequent underground hacker forums.

KrebsOnSecurity.com spoke to that reseller. In exchange for the agreement that I not name his operation or his location, he provided payment information about the customer who purchased dozens of servers that were used to manipulate the day-to-day operations of the massive botnet.

The reseller was willing to share information about his client because the customer turned out to be a deadbeat: The customer walked out on two months worth of rent, an outstanding debt of $1,600. The reseller also seemed willing to talk to me because I might be able bend the ear of **Spamhaus.org**, the anti-spam group that urged ISPs worldwide to block his Internet addresses (several thousand dollars worth of rented servers) shortly after Microsoft announced the Rustock takedown.

I found the reseller advertising his services on a Russian-language forum that caters exclusively to spammers, where he describes the hardware, software and connection speed capabilities of the very servers that he would later rent out to the Rustock botmaster. That solicitation, which was posted on a major spammer forum in January 2010, offered prospective clients flexible terms without setting too many boundaries on what they could do with the servers. A translated version of part of his message:

> “I am repeating again that the servers are legitimate, funded by us and belong to our company. To the datacenters, we are responsible to ensure that you are our client, and that you will not break the terms of use. Also, to you we are responsible to make sure that the servers are not going to be closed down because of credit card chargebacks, as it happens with servers funded with stolen credit cards. In conclusion, they do not have an abuse report center, they are suitable for legitimate projects, VPNs and everything else that does not lead to problems and complaints to the data center from active Internet users. Please, take it in consideration, so that nobody is pissed off and there is no bad impression from our partnership.”

The reseller said he had no idea that his customer was using the servers to control the Rustock botnet, but he hastened to add that this particular client didn’t attract too much attention to himself. According to the reseller, the servers he resold to the Rustock botmaster generated just two abuse complaints from the Internet service providers (ISPs) that hosted those servers. Experts say this makes sense because botnet control servers typically generate few abuse complaints, because they are almost never used for the sort of activity that usually prompts abuse reports, such as sending spam or attacking others online. Instead, the servers only were used to coordinate the activities of hundreds of thousands of PCs infected with Rustock, periodically sending them program updates and new spamming instructions.

The reseller was paid for the servers from an account at WebMoney, a virtual currency similar to PayPal but more popular among Russian and Eastern European consumers. The reseller shared the unique numeric ID attached to that WebMoney account — WebMoney purse “Z166284889296.” That purse belonged to an “attested” WebMoney account, meaning that the account holder at some point had to verify his identity by presenting an official Russian passport at a WebMoney office. A former law enforcement officer involved in the Rustock investigation said the name attached to that attested account was “Vladimir Shergin.” According to the reseller, the client stated in an online chat that he was from Saint Petersburg, Russia.

A LUCRATIVE PILL-PUSHING MACHINE

As it happens, that same WebMoney account is connected to three of the top promoters of “SpamIt,” a rogue pharmacy program that paid spammers millions of dollars to promote fly-by-night sites that sold counterfeit prescription drugs. SpamIt closed its doors in September 2010 when its alleged leader came under scrutiny from Russian authorities. The SpamIt financial books sent to me by an anonymous source last year include the ICQ numbers, phone numbers and financial account information for hundreds of established criminal hackers and spammers. The SpamIt accounts show that a promoter using the nickname “**Cosma2k**” who used that WebMoney account was consistently among the top 10 moneymakers for SpamIt, and that he earned more than a half-million dollars in commissions over the course of three years with the pharmacy program.

Yet this appears to be only a fraction of Cosma2k’s total earnings through SpamIt. The pharmacy program’s records show that a Cosma2k affiliate also used at least one other WebMoney account that was shared with two other top SpamIt members, accounts tied to the user names **“Bird**” and **“Adv1**.” A review of the account details for all three affiliates show they also all provided the same ICQ number at time of registration. The total commissions from all three user accounts at SpamIt was nearly $2.14 million over three-and-a-half years.

But that’s not all: Those same three affiliate names — Cosma2k, Bird and Adv1 — also were registered using the same ICQ account at **Rx-Promotion**, a competing rogue Internet pharmacy program. Rx-Promotion suffered a security breach last year in which its affiliate records were taken. A copy of those records was shared with KrebsOnSecurity.com, and they show that these three accounts collectively earned approximately $200,000 in commissions by promoting pharmacy Web sites for Rx-Promotion in 2010.

If Cosma2k really is responsible for Rustock, the payment data suggests either that he was sharing control over the botnet with others, or that he split his promotion activities across multiple accounts, perhaps to keep legions of other affiliates from feeling resentful of his earnings and to avoid calling undue attention to any one account. In fact, the SpamIt account belonging to Bird was by far the highest earning affiliate account in the entire history of program, and Bird routinely earned twice as much in commissions as the next most successful affiliate (which often enough was either Cosma2k or Adv1). In January 2010, for example, the SpamIt records show Bird’s spam generated more than $130,000 in pharmacy sales, while the next most successful affiliate for that month realized about $86,000 in sales.

Alex Lanstein, a network architect at **FireEye**, a Milpitas, Calif. based security firm that worked closely with Microsoft on the Rustock takedown, said he doubts there were multiple people responsible for running Rustock.

In fact, Lanstein said, bots such as ZeuS and Mega-D have shown that it doesn’t take more than one coder to be wildly successful. “Most people probably assume that to be wildly successful in the world of botnets, you need to have a huge team of programmers. Most malware these days is specialized with only one or two real functions built-in,” Lanstein said. “Why incur of the overhead of splitting profits when a bot operator can pay one-time fees to a 3rd party service and keep the real profit for yourself?”

“Unfortunately the barrier for entry into the malware game is extremely low, and when extradition is difficult, and the criminals avoid affecting computers in their own country, the burden on law enforcement is extreme.”

SOFTWARE GIANT SEEKS BOTMASTER FOR COURTROOM DRAMA

Microsoft also was in communication with my informant reseller, and obtained much of the same data as I did. And the company plans to soon publish at least some of the information, albeit in a rather unusual way. According to **Richard Boscovich**, senior attorney for Microsoft’s Digital Crimes Unit, the software giant seized the Rustock control servers by securing what’s known as an *“ex parte* temporary restraining order,” which allowed Microsoft to take down the botnet without giving the defendants advance notice.

But Microsoft is required by law to now make a “good faith effort” to contact the owner(s) of Rustock control domains and other infrastructure the company has since seized, and to notify the individual(s) of the date, time and location of an upcoming court hearing in Seattle, Washington, where the defendants will have an opportunity to be heard.

Microsoft will publish the information on a Web site set up for this purpose – noticeofpleadings.com. The company may also seek to publish the information in one or more major Russian newspapers, Boscovich said.

“We will have to send out a notice to the individual or [group of] individuals we believe is behind the bot,” Boscovich said. “We will probably also serve notice of process in Russian newspapers or in a Saint Petersburg newspaper, saying ‘Hey, Mr. Such-and-Such, there is a court hearing in Seattle on this case and we expect you to be there.'”

It will be interesting to see who, if anyone, responds to the Microsoft notices, and whether the veil of anonymity will be lifted from the pseudonyms of botmasters, spammers, and account holders. Stay tuned!