Korplug RAT используется в направленных атаках на пользователей Афганистана и Таджикистана

Korplug RAT представляет из себя средство удаленного доступа, которое также известно как **PlugX**. Недавно мы обратили более пристальное внимание на кампании злоумышленников по распространению этой вредоносной программы. Одна из таких кампаний используется для проведения направленных атак на Афганистан и Таджикистан.

Зачастую, в направленных атаках, злоумышленники прибегают к услугам новых модификаций вредоносного ПО. В дальнейшем, обнаружение такого вредоносного ПО может помочь однозначно идентифицировать источник атаки, т. е. киберпреступную группу. В качестве примера можно взять последнюю модификацию вредоносной программы **BlackEnergy** (BlackEnergy Lite aka BlackEnergy 3). Эта модификация использовалась в направленных атаках на Украину и страны Восточной Европы группой киберпреступников под названием Quedagh или Sandworm. Она явно отличалась от своей предыдущей второй версии, многочисленные файлы которой до сих пор можно встретить на компьютерах пользователей.

В других случаях, атакующие используют более распространенные инструменты для достижения своих преступных целей. Например, **Korplug RAT**, который представляет из себя широко известный вредоносный инструмент, неоднократно использовался китайскими APT-группами, начиная с 2012 г., для проведения направленных атак. Последние несколько недель мы наблюдали большое количество обнаружений **Korplug** во многих не связанных между собой инцидентах.

Среди этих случаев заражений мы смогли обнаружить несколько успешных инфекций, где используемые образцы **Korplug** взаимодействовали с одним C&C-сервером.

```
DOMAIN: www.notebookhk.net
Updated Date: 2013-11-12 18:03:45
Create Date: 2013-06-18 11:08:17
Registrant Name: lee stan
Registrant Organization: lee stan
Registrant Street: xianggangdiqu
Registrant City: xianggangdiqu
Registrant State: xianggang
Registrant Postal Code: 796373
Registrant Country: HK
Registrant Phone : +0.04375094543
Registrant Fax: +0.04375094543
Registrant Email:stanlee@gmail.com
```

Другие образцы вредоносной программы взаимодействовали с C&C-серверами, адреса которых отличаются от вышеупомянутого, однако, они принадлежат одному IP-адресу.

```
DOMAIN: www.dicemention.com
Updated Date: 2013-11-12 18:05:33
Create Date: 2013-09-10 14:35:11
Registrant Name: z x
Registrant Organization: z x
Registrant Street: xianggangdiqu
Registrant City: xianggangdiqu
Registrant State: xianggang
Registrant Postal Code: 123456
Registrant Country: HK
Registrant Phone : +0.0126324313
Registrant Fax: +0.0126324313
Registrant Email: 123@123.com

DOMAIN: www.abudlrasul.com
Updated Date: 2014-10-16 14:16:27
Create Date: 2014-10-16 14:16:27
Registrant Name: gang xin
Registrant Organization: gang xin
Registrant Street: Argentina Argentina
Registrant City: Argentina
Registrant State: Argentina
Registrant Postal Code: 647902
Registrant Country: AR
Registrant Phone : +54.0899567089
Registrant Fax: +54.0899567089
Registrant Email: woffg89@yahoo.com
```

Взяв эти адреса C&C-серверов в качестве отправной точки, мы смогли обнаружить определенное число жертв вредоносной программы, которые были заражены с использованием различных поддельных документов. Эти документы рассылались в фишинговых сообщениях и содержали в себе эксплойты. Кроме этого, для этой же цели использовались самораспаковывающиеся RAR-архивы с расширением .SCR.

Имя файла	SHA1
Situation Report about Afghan.doc	36119221826D0290BC23371B55A8C0E6A84718DD
AGREEMENT BETWEENTHE NATO AND AFGHANISTAN ON THE STATUS OF NATO FORCES IN AFGHANISTAN.doc	A6642BC9F3425F0AB93D462002456BE231BB5646
news.doc	51CDC273B5638E06906BCB700335E288807744B5
План деятельности соединений и воинских частей Приволжского региона на июль 2014 г.scr	EA6EE9EAB546FB9F93B75DCB650AF22A95486391
телефонный справочник структуры МИД КР .scr	D297DC7D29E42E8D37C951B0B11629051EEBE9C0
О Центре социальной адаптации военнослужащих.scr	8E5E19EBE719EBF7F8BE4290931FFA173E658CB8
Протокол встречи НГШ КНР.scr	1F726E94B90034E7ABD148FE31EBA08774D1506F
исправленный шаблон плана мероприятий.scr	A9C627AA09B8CC50A83FF2728A3978492AEB79D8
Situation Report about Afghan.scr	A9C627AA09B8CC50A83FF2728A3978492AEB79D8
Военно-политическая обстановка в ИРА на04.10.2014.scr	E32081C56F39EA14DFD1E449C28219D264D80B2F
Afghan Air Force.scr	E32081C56F39EA14DFD1E449C28219D264D80B2F
план мероприятий.scr	1F726E94B90034E7ABD148FE31EBA08774D1506F

Фальшивый документ может иметь следующий вид.

AGREEMENT BETWEENTHE NORTH ATLANTIC TREATY ORGANIZATION AND THE ISLAMIC REPUBLIC OF AFGHANISTAN ON THE STATUS OF NATO FORCES AND NATO PERSONNEL CONDUCTING MUTUALLY AGREED NATO-LED ACTIVITIES IN AFGHANISTAN

The North Atlantic Treaty Organization, hereinafter NATO represented by His Excellency Mr. MauritsR.JochemsNATO Senior Civilian Representative in Afghanistan,and The Islamic Republic of Afghanistan, hereinafter Afghanistan represented by His Excellency Mr.Mohammed Haneef AtmarNational Security Advisor,hereinafter referred to as the "Parties",Considering that, in the 2012 Chicago SummitDeclaration on Afghanistan, the Heads ofState and Government of the Islamic Republic of Afghanistan and the nations contributingto the International Security Assistance Force (ISAF) renewed their firm and sharedcommitment to a sovereign, secure and democratic Afghanistan;Confirming the shared understanding of the Parties of the threat to the internationalcommunity posed by terrorism and their shared commitment to taking effective action tocounter that threat and to ensuring that Afghanistan never again becomes a safe haven forterrorists;Recognizing that the mission of the ISAF will be concluded by the end of 2014;Recalling the commitment of NATO and other members of the international community tostanding with Afghanistan and the Parties'agreement at the NATO Summit in Lisbon torenewing and building a robust Enduring Partnership complementing their past securitycooperation and continuing beyond it;Affirming the Parties' intention that this Enduring Partnership include an individualprogramme of co-operation activities with security ministries and other national institutionsand on enhancing the capabilities and skill levels in the Afghan security forces, includingtheir ability to tackle the threats of terrorism, through training and supporting specialisedAfghan units and appropriate access to NATO courses, institutions and military and civilianexpertise;and Reaffirming, finally, the Parties' agreement on the value of NATO leading a non-combat,training, advising and assisting mission in Afghanistan beginning after 2014;Have agreed as follows:

ARTICLE 1

Definitions

1. "NATO" means the North Atlantic Treaty Organization, its subsidiary bodies, itsmilitary headquarters, all its constituent national elements/units and the constituentnational elements/units from Operational Partners.

2. "NATO Member States" are currently Albania, Belgium, Bulgaria, Canada, Croatia,the Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy,Latvia, Lithuania, Luxembourg, the Netherlands, Norway, Poland, Portugal, Romania,Slovakia, Slovenia, Spain, Turkey, the United Kingdom and the United States.

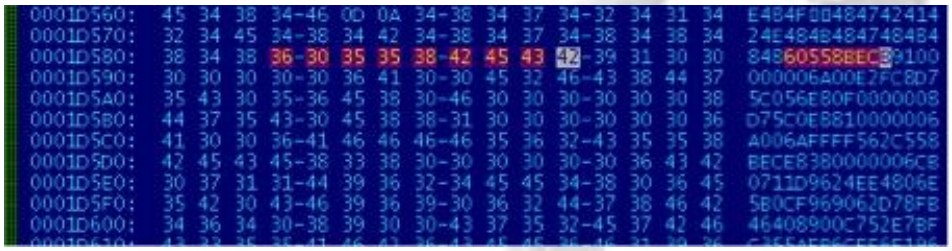
3. "Operational Partners" means states other than NATO member states that,following close consultations3.1,have been agreed to and accepted by the government of

Во всех этих случаях, в результате успешной эксплуатации уязвимости, на диск записываются три новых файла, при этом происходит загрузка в память вредоносного компонента **Korplug**.

- exe – легитимный исполняемый файл, который подписан цифровой подписью одной из security-компаний (легитимный файл), и загружает в память динамическую библиотеку;
- dll – небольшой загрузчик, выполненный в виде динамически подключаемой библиотеки;
- dll.avp – файл с исполняемым кодом **Korplug**.

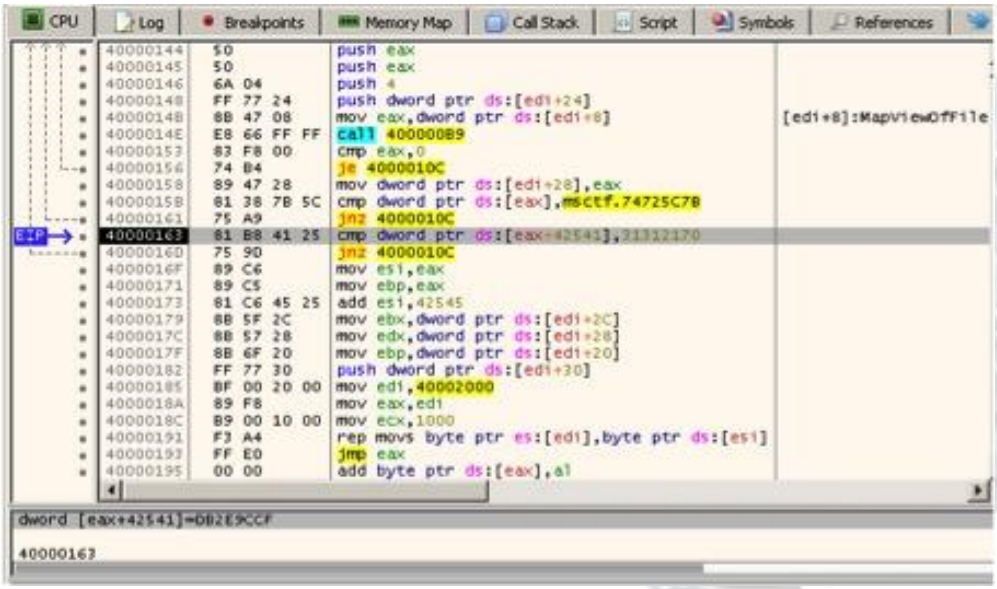
Вредоносное ПО **Korplug RAT** использует специальный метод для обмана AV-продуктов, который заключается в использовании исполняемого файла какого-либо security-продукта, который позволяет загрузить указанную извне динамическую библиотеку в память.

Указанные выше документы в формате RTF представляют из себя эксплойты для уязвимости **CVE-2012-0158** в MS Word. Скриншот ниже показывает начало шелл-кода эксплойта к этой уязвимости, указанные ASCII-символы соответствуют инструкциям *pusha; push ebp; mov ebp, esp*.



Интересно отметить, что эти документы также содержат эксплойт к более новой уязвимости **CVE-2014-1761**, которая уже неоднократно использовалась злоумышленниками в направленных атаках для доставки таких вредоносных программ как BlackEnergy, Sednit, MiniDuke, и др. Однако, этот эксплойт был разработан некорректно и содержал неверный указатель в инструкциях шелл-кода.

Ниже на скриншоте мы видим инструкции шелл-кода, который исполняется на первой стадии работы эксплойта. Инструкции проверяют присутствие тэга «p!11», с которого начинаются новые инструкции второй стадии шелл-кода. После этого он пытается загрузить их в память. Даже в случае присутствия этого тэга и шелл-кода в памяти, он расположен по другому смещению, т. е. отличному от того, которое пытается использовать вредоносная программа.



Мы смогли обнаружить жертв **Korplug** в следующих странах.

- Афганистан
- Таджикистан
- Россия
- Кыргызстан
- Казахстан

Из темы указанных выше документов, которые использовались для распространения вредоносных программ, можно утверждать, что атакующих интересовал сбор разведывательной информации на военную и дипломатическую темы. Также можно отметить следующую закономерность: на компьютерах жертв были найдены другие вредоносные программы, в т. ч. инструменты удаленного доступа (RAT), троянские программы, кейлоггеры. Одна из этих вредоносных программ взаимодействовала с удаленным сервером, доменный адрес которого совпадал с аналогичным адресом, который использовался в образцах **Korplug**.

Поскольку возможности этих вредоносных программ частично перекрывались с возможностями **Korplug**, для нас не совсем ясно почему они использовались злоумышленниками. Возможно, они просто экспериментировали с различными типами вредоносных программ или использовались для выполнения тех задач, которые нельзя выполнить функциями **Korplug**. Вместе с **Korplug**, на зараженных компьютерах, чаще всего встречались два нижеуказанных семейства вредоносных программ.

DarkStRat

Эта вредоносная программа также представляет из себя еще один инструмент удаленного доступа (RAT). Его исследование показывает связь **DarkStRat** с Китаем и Испанией. В частности, команды отдаваемые боты написаны на испанском языке. В скобках указан их перевод на английский язык.

- CERRAR (закрыть)
- DESINSTALAR (удалить)
- SERVIDOR (сервер)
- INFO
- MAININFO
- PING
- REBOOT

- POWEROFF
- PROC
- KILLPROC
- VERUNIDADES (просмотр юнитов)
- LISTARARCHIVOS (получить список файлов)
- EXEC
- DELFILE
- DELFOLDER
- RENAME
- MKDIR
- CAMBIOID (изменить идентификатор)
- GETFILE/SENDFILE/RESUMETRANSFER
- SHELL
- SERVICIOSLISTAR (получить список сервисов)
- INICIARSERVICIO (запустить сервис)
- DETENERSERVICIO (остановить сервис)
- BORRARSERVICIO (удалить сервис)
- INSTALARSERVICIO (установить сервис)

Вредоносные программы **DarkStRat** могут управлять процессами и сервисами на зараженной машине, передавать файлы на удаленный сервер и копировать их оттуда, исполнять инструкции командного интерпретатора и т. д. Для написания **DarkStRat** использовался язык Delphi, одна из модификаций подключается к домену www.dicemention.com. Также некоторые образцы этого вредоносного ПО имеют цифровую подпись компании «Nanning weiwu Technology co.,ltd».

File Stealer

Еще один тип вредоносного ПО, который часто встречался с **Korplug**. Эта вредоносная программа написана на языке C и содержит функции по краже файлов с жестких дисков зараженных компьютеров. Список таких файлов указан в специальном конфигурационном файле. Кроме рекурсивного поиска этих файлов на жестких дисках, он способен отслеживать подключение к системе съемных носителей и сетевых папок, ожидая специальное системное событие DBT_DEVICEARRIVAL.

В дополнении к его функциям кражи файлов и передачи их на удаленный сервер злоумышленников, эта вредоносная программа специализируется на похищении сохраненных пользователем на компьютере паролей от различных интернет-аккаунтов, а также списка посещенных пользователем в браузере URL-адресов и информации об используемых аккаунтов следующих приложений.

- Microsoft Messenger
- Microsoft Outlook
- Microsoft Internet Explorer
- Mozilla Firefox

Вредоносная программа использует следующие домены для связи с управляющим C&C-сервером.

- newvinta.com
- worksware.net

Некоторые образцы этого File Stealer подписаны уже упомянутым цифровым сертификатом, выданным компанией «Nanning weiwu Technology co.,ltd».