**Cyber Security Fundamentals**

**Sality Virus research**

**Выполнил: Мұхаметқазин Э.Т.**

**Проверил: Иманбаев А.Ж.**

**Алматы 2019**

**Название вируса: Sality**

Sality — одно из наиболее известных семейств вредоносного программного обеспечения. В своем развитии ВПО Sality прошло несколько стадий. Virus.Win32.Sality.aa - файловый вирус. Заражает исполнимые \*.exe файлы размером более 100 кб с увеличением их длины. Иконка файла сохраняется. Вирус заражает файлы, которые запускаются пользователем (иногда вместо заражения файл портится и после этого не запускается), и некоторые случайные файлы.Sality пытается внедрить свою копию во все запущенные процессы, за исключением тех, которые выполняются от имени аккаунтов 'system', 'local service' и 'network service'. Для привилегированных процессов выставляет себе Debug privileges, и пытается внедриться снова. Для исключения повторного внедрения использует mutex с именем приложения. Это является одним из признаков инфицирования компьютера. Защитный модуль защищает Sality от антивирусного ПО. Для предотвращения загрузки ОС в режиме защиты от сбоев (Safe boot mode) вирус удаляет из реестра ключи и значения в следующих ветках: 'HKEY\_CURRENT\_USER\System\CurrentControlSet\Control\SafeBoot' и 'HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SafeBoot'.  
Блокируется работа служб множества антивирусных программ. Ранние версии Sality вели себя даже более агрессивно и просто удаляли эти службы из системы.  
Вирус также внедряет драйвер ядра. Этот драйвер добавляется под псевдослучайным именем в папку %System%\drivers. Создается служба с именем «amsint32».

Я заметил что с диска С удалились файлы (высылаю фото до и после). Потом зашел в Autorun и заметил процесс вирусного типа, и решил еще раз проверить и зашел в Process Explorer. И точно удостоверился что на компе вирус. Я оттуда узнал где находится exe файл вируса, захэшировал ее с помощью HashCalc, и вбил его хэш в Total Process.Чтобы определить вирус мы скачали программу DR Web, потом сделал Kill Process в Process Explorer. Но чтобы удостовериться что окончательно вылечил я узнал какой вирус, потом вбил в интернете как лечить этот вирус. Там вышли разные способы лечения и утилиты для этого. Я воспользовался DoctorWeb и вылечил.